@ISACA
RELEVANT, TIMELY NEWS
Volume 6, 12 March 2014

Wearable Technology and Its Associated Security Risk

By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP

One of the fastest growing facets of the technology field is wearable technology. Currently, wearable technology can be broken into 2 major categories: health monitors and smartwatches. Each poses unique security challenges. The known vulnerabilities associated with wearable technology are found in the software that users load onto workstations and the devices themselves.

Read More

Speaker Spotlight: Learn to Use Privacy Principles for Business Benefit

Learn from one of the world's leading privacy specialists at the 2014 North America CACS. Rebecca Herold, CISA, CISM, has been named one of the best privacy advisors in the world by *Computerworld* magazine multiple times. She is the author of 15 books and hundreds of articles on the subject of information security and privacy.

Read More

Defend Your Enterprise From Increasingly Advanced Cyberattacks

In recent months, advanced persistent threats (APTs) have become much more sophisticated and damaging. Modern APTs have the ability to easily extract information from databases. Given the highly sophisticated nature of these cyberattacks, it is imperative that security professionals learn as much as possible to combat and conquer them.

Read More

Your Unique ISACA Member Benefit—COBIT 5

As a member of ISACA®, you have access to COBIT® 5, which provides the only end-to-end business view of governance of enterprise IT (GEIT). COBIT 5 reflects the central role of information and technology in creating value for enterprises.

Read More

Funding Available as New CSR Program Kicks Off

ISACA's new corporate social responsibility (CSR) program began in January 2014 and will operate for 3 years on a pilot basis. Perhaps of most direct interest to members and chapters is the portion of the program that enables chapters, volunteers, members and staff to apply for funding from ISACA to support local/regional organizations and activities.

Read More

ISACA Certifications Top the List of Highest Paying Certifications

ISACA certifications help you become more valuable to your organization. A recent report by Global Knowledge lists CRISC™, CISM® and CISA® as being among the top paying certifications in 2014, finishing first, second and third, respectively.

Read More

Growing Personally and Professionally Through ISACA Involvement

Mustafa Lotia, CISA, CISO, Information Governance & Compliance Manager at InfoFort, Shares His Experience as a CISA

For Mustafa Lotia, pursuing the CISA certification was a necessary step in his career. “In the United Arab Emirates (UAE), it is becoming more of a requirement if you wish to be in the IS audit domain. Professionally, it has added a lot more value than anticipated initially, as I have become a subject matter specialist not only as a certified IS auditor, but also at each technology/business program we embarked upon.”

Read More

Book Review: *Computer Forensics*

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

Computer Forensics is primarily aimed at individuals who have technical knowledge of computers and want to pursue a career in computer forensics. It is a distillation of author David Cowen’s knowledge and experience from more than 14 years in the field. Cowen has been practicing computer forensics since 1999 and testifying as an expert witness since 2003.

Read More

Wearable Technology and Its Associated Security Risk

By Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP

A woman whose security manager had banned all wearable technology from their facility recently confronted me during my Christmas vacation. She was outraged that her expensive pedometer could not be worn at work. “What’s the threat? What’s the vulnerability?” And most important, she asked, “Why are you security people so paranoid?” The fast answer, of course, is: “We are paid to be paranoid.”

One of the fastest-growing facets of the technology field is wearable technology. Currently, wearable technology can be broken into 2 major categories: health monitors and

smartwatches. Each poses unique security challenges. The known vulnerabilities associated with wearable technology are found in the software that users load onto workstations and the devices themselves. These weaknesses allow ill-intentioned actors to see and modify the individual performance reported by the device. However, in every case, the testers would need a privileged account to take advantage of the vulnerabilities.

The devices themselves have vulnerabilities that are easily mitigated using compensating controls. Both types of wearable technology are Bluetooth-enabled. The fear is that these devices can connect to unprotected Bluetooth emitters and begin to receive data. In addition, the device could be modified to become a data vacuum, even though no record of that exists (yet). This is more likely to happen to a smartphone, since it acts more like a computer, than a health monitor, a single-function device. Plus, if this is the vulnerability you are preventing, you may have a bigger issue with personnel. Smartwatches can also have a camera, which presents a known issue for a lot of secure locations.

The following are some general tips for wearable technology:

1. Allow wearable technology anywhere mobile phones are allowed.
2. Ensure workstations and other technology are configured so that random Bluetooth requests cannot pair.
3. Maintain your software baseline on technology:
    - Validate workstation baselines to ensure unapproved software is not present.
    - Ensure your software baseline does not allow installation of wearable technology clients.
4. Develop a policy that distinguishes smartwatches from health monitors:
    - Bluetooth should be an acceptable risk if compensating controls are in place.
    - Cameras should not be allowed in high-assurance areas.

In the end, be cautious with wearable technology. It is easy to write policies that lead to overprotection. Health monitors, as single-function devices, are harder to modify and, thus, misuse than smartwatches. In the example cited previously, the main reason the wearable technology was being banned was for its routing ability. The capability to route using this technology is no greater threat than a bad actor drawing out the floor plan and showing exactly where strategic people are located within the office space.

Returning to the initial example, with an open-source search, I was able to find the floor plan, HVAC, power and overall secure campus, measured to inches, of her corporate workplace in less than 10 minutes. After ghost writing an email to her security office, the security officer is looking to rescind the previous policy on this subject in lieu of a more reasonable approach. The public availability of this kind of information makes the main reason for banning wearable technology moot.

Additional information on creating policies for mobile devices can be found in ISACA's *Securing Mobile Devices Using COBIT 5 for Information Security*, which is available in the

ISACA Bookstore and is a free member download from the **Knowledge Center**.

Bruce R. Wilkins, CISA, CISM, CGEIT, CRISC, CISSP, is the chief executive officer of TWM Associates Inc. In this capacity, Wilkins provides secure engineering solutions for innovative technology and cost-reducing approaches to existing security programs.

Speaker Spotlight: Learn to Use Privacy Principles for Business Benefit

Learn from one of the world's leading privacy specialists at the 2014 North America Computer Audit, Control and Security (CACS) Conference. Rebecca Herold, CISA, CISM, has been named one of the best privacy advisors in the world by *Computerworld* magazine multiple times. She is the author of 15 books and hundreds of articles on the subject of information security and privacy. Herold will lead a postconference workshop on Wednesday, 30 April, titled "Using Privacy Principles Within Business."

Workshop attendees will benefit from Herold's decades of experience in the field. The workshop will provide attendees the tools needed to perform privacy impact assessments, identify their organization's privacy needs, and determine the best framework for their organization's business goals and objectives.

Herold is chief executive officer (CEO) of Privacy Professor, a partner at Compliance Helper and adjunct professor for the Norwich University (Northfield, Vermont, USA) Master of Science in Information Security and Assurance program. She has received a plethora of accolades for her knowledge of information security, including being named a Privacy by Design Ambassador by the Ontario (Canada) Data Privacy Commissioner.

Learn more about this session and others planned for the upcoming **North America CACS**, being held in Las Vegas, Nevada, USA, on 28-30 April 2014.

Defend Your Enterprise From Increasingly Advanced Cyberattacks

In recent months, advanced persistent threats (APTs) have become much more sophisticated and damaging. Modern APTs have the ability to easily extract information from databases.

Given the highly sophisticated nature of these cyberattacks, it is imperative that security professionals learn as much as possible to combat and conquer them.

Learn more about defending your organizations from these threats. Attend ISACA's free virtual conference, Cybersecurity: Collaborate, Comply, Conquer, on Tuesday, 18 March from 7:15 a.m. to 4:00 p.m. CDT (UTC-5).

This conference will give you the opportunity to learn from subject matter experts who have first-hand experience with APTs. As an attendee, you will be equipped with the tools and insights to combat increasingly advanced global threats and prepare for regulatory changes that will affect cybersecurity professionals around the world. In addition, participants can earn 5 free certified professional education (CPE) hours for attending.

To register or learn more about the sessions offered, visit the **Cybersecurity: Collaborate, Comply, Conquer** page of the ISACA web site.

Your Unique ISACA Member Benefit—COBIT 5

As a member of ISACA®, you have access to COBIT® 5, which provides the only end-to-end business view of governance of enterprise IT (GEIT). COBIT 5 reflects the central role of information and technology in creating value for enterprises. Your ISACA membership gives you access to the latest thinking on enterprise governance and management. COBIT 5, now available for download in 12 languages from the COBIT 5 **Product Family** page of the ISACA web site, provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

Many COBIT 5 products are free to members, including COBIT 5, *COBIT® 5: Enabling Processes, COBIT® 5: Enabling Information* and *COBIT® 5 Implementation*. Professional guides specific to each field, such as *COBIT 5® for Information Security, COBIT® 5 for Assurance* and *COBIT® 5 for Risk*, are available at discounted rates for members. Download your copies today on the **COBIT 5** page of the ISACA web site.

In addition, ISACA research supports the development and understanding of COBIT, connecting you with the tools to advance your thought leadership. The **Deliverables** page contains the latest ISACA publications—free to members—including *Configuration Management Using COBIT® 5* and *Transforming Cybersecurity Using COBIT® 5*.

You can also connect with more than 110,000 professionals from across the globe by posting comments and asking questions about COBIT 5 in the **Knowledge Center**. For more information about COBIT 5 and your membership benefits, please contact **membership@isaca.org**.

Funding Available as New CSR Program Kicks Off

ISACA's new corporate social responsibility (CSR) program began in January 2014 and will operate for 3 years on a pilot basis. A volunteer working group, consisting of representatives from the Chapter Support Committee, the Finance Committee and the Relations Board, developed criteria for various types of giving to be undertaken by the program.

Perhaps of most direct interest to members and chapters is the portion of the program that enables chapters, volunteers, members and staff to apply for funding from ISACA® to support local/regional organizations and activities. The criteria to qualify for funding and a link to the application form are available on the **Criteria for Support of a Cause** page of the ISACA web site. Examples of the types of organizations that might qualify include Code.org, Internet Watch Foundation, Mentornet or Minds Matter. Donations in support of providing laptops to underprivileged schools or cybersecurity awareness days/months are activities that may also qualify for funding. A local/regional angle is encouraged for these activities so that the funding is focused in the area in which the chapter or member resides. An activity that offers chapters/members an opportunity to participate (e.g., mentor students, deliver/set up laptops)—in addition to the funding—is even better. The volunteer working group will review all submissions.

The program's other contributions include:

- ISACA will donate to 1 or more international organizations selected by the working group annually. Two organizations have been identified for 2014; their names will be announced once contact has been made and the details surrounding the donations have been finalized.
- ISACA will donate to relief agencies in areas significantly affected by natural or man-made disasters. (ISACA has been doing this for several years; the CSR program formalizes the process.)

Visit the **Corporate Social Responsibility Program** page on the ISACA web site for further details on the donation criteria. Questions? Contact **csr@isaca.org**.

ISACA Certifications Top the List of Highest Paying Certifications

ISACA® certifications help you become more valuable to your organization. In 2013, ISACA certified more than 6,900 Certified Information Systems Auditors (CISAs), 2,600 Certified

Information Security Managers (CISMs), 450 Certified in the Governance of Enterprise IT (CGEITs) and 650 Certified in Risk and Information Control (CRISCs).

A **recent report by Global Knowledge** lists CRISC™, CISM® and CISA® as being among the top paying certifications in 2014, finishing first, second and third, respectively.

Becoming certified requires passing an exam and having experience in the field. **CISA**, **CISM**, **CGEIT®** and **CRISC** certification requirements can be found on the ISACA web site.

The final registration date for the June 2014 exam is 11 April 2014. Please make note that in 2014, the CISA German-, Hebrew- and Italian-language exams are available only at the June exam administration. The June 2014 exam registration can be completed on the **Exam Registration** page of the ISACA web site.

Growing Personally and Professionally Through ISACA Involvement

Mustafa Lotia, CISA, CISO, Information Governance & Compliance Manager at InfoFort, Shares His Experience as a CISA

For Mustafa Lotia, pursuing the Certified Information Systems Auditor® (CISA®) certification was a necessary step in his career. “In the United Arab Emirates (UAE), it is becoming more of a requirement if you wish to be in the IS audit domain. Professionally, it has added a lot more value than anticipated initially, as I have become a subject matter specialist not only as a certified IS auditor, but also at each technology/business program we embarked upon.”

In addition to his CISA certification, Lotia has been on the board of directors for the ISACA® UAE Chapter for the past 3 years. He became the chapter certification director in 2013, and he organizes review classes for all ISACA certifications. His CISA certification and involvement with ISACA has given Lotia the opportunity to meet new people and learn in a nontraditional way. “I love to socialize with people from different aspects of life,” he says. “It drives your knowledge base…knowledge that you may not get from traditional academics. I love the role of interactive trainer, as I learn a lot from my audiences.”

Lotia’s personal goals and professional goals are intertwined, and obtaining the CISA certification helped him achieve these goals. “To me, personal goals are the sizeable force in mentoring your professional goals. In my case, I always wanted to be in an advisory role, so I embarked on the domain of governance and compliance. CISA definitely added value.

Maintaining your certification means your personal goals will not expire and you will always remain in the desired community."

To anyone interested in pursuing the CISA certification, Lotia says, "If you want to be recognized and respected in the IS audit domain, just try it! You won't regret it."

To learn more about ISACA certifications, visit the **Certification** page of the ISACA web site.

Book Review: *Computer Forensics*

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

Computer Forensics is primarily aimed at individuals who have technical knowledge of computers and want to pursue a career in computer forensics. It is a distillation of author David Cowen's knowledge and experience from more than 14 years in the field. Cowen has been practicing computer forensics since 1999 and testifying as an expert witness since 2003.

Although the book is geared toward people interested in taking their first steps into computer forensics, it will also appeal to a wider audience. Auditors and security professionals alike will find it interesting reading should they need to employ a forensic expert or oversee an investigation.

The book, which delivers content in a clear and straightforward manner, is laid out as a how-to guide to becoming involved in computer forensics and is split into 4 sections: Getting Started, Your First Investigation, How to Work a Case and Defending Your Work. This book provides as much emphasis on what might be considered the more mundane aspects of computer forensics, such as the importance of good procedures and documentation, as it does on forensic discovery.

Computer Forensics clearly covers training, certification and tools, but leaves it to readers to make their own judgment about the value of these programs.

The publication provides the reader with a single point of reference for starting computer forensics. For a relatively short book, considering the subject matter (318 pages), it contains essential information on computer forensics. Each chapter contains numerous references to external information, tools and documentation. The author also maintains an accompanying blog that contains tools, documentation, video tutorials and example images that can be used when practicing forensic techniques.

It is important to note that the publication's content regarding professional licensing requirements, litigation and reports for courts and exhibits is US-centric, based on the author's experience within the boundaries of the US legal system. The book does point out that readers should research the legal system in which they will be working.

Computer Forensics is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in the latest issue of the ***ISACA Journal***, visit the **ISACA Bookstore** online or email **bookstore@isaca.org**.

Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI, is the group information security officer (ISO) at AEGON UK. Richardson has more than 25 years of experience in IT, information security, audit and risk.