Volume 4, 2016

ISACA Journal

# mobile apps

Mobile Payments as a Security Control?

Mobile App Security Audit Framework

Benefits and the Security Risk of Software-defined Networking

www.isaca.org

ISACA®

*Trust in, and value from, information systems*

SHOWCASE YOUR EXPERTISE—START BY REGISTERING FOR AN ISACA CERTIFICATION EXAM TODAY!

# "WHEN YOU GET CERTIFIED, **YOU GET RECOGNIZED**. THAT MAKES OTHERS **RESPECT YOUR OPINIONS**."

— ROSEMARY AMATO, CISA
DIRECTOR, DELOITTE
AMSTERDAM, THE NETHERLANDS
ISACA MEMBER SINCE 1998

Holding an ISACA® certification validates your expertise, increases your earning potential and expands your opportunities. **Register for an upcoming exam today!**

Register at *www.isaca.org/2016exams-Jv4*

ACCOMPLISH MORE

## UPCOMING CERTIFICATION EXAMS

**10 September 2016***
Final Registration Deadline: 22 July 2016
* CISA and CISM only

**12 December 2016**
Early Registration Deadline: 19 August 2016
Final Registration Deadline: 21 October 2016

CISA® Certified Information Systems Auditor®

CISM® Certified Information Security Manager®

CGEIT® Certified in the Governance of Enterprise IT®

CRISC™ Certified in Risk and Information Systems Control™

ISACA®
*Trust in, and value from, information systems*

Hurry—register early for a Decmeber exam to save US $50!

***www.isaca.org/2016exams-Jv4***

Learn the essentials of managing compliance & ethics programmes

INTERNATIONAL

# BASIC COMPLIANCE & ETHICS ACADEMIES

FROM THE SOCIETY OF CORPORATE COMPLIANCE & ETHICS®

**11–14 JULY, 2016** | SINGAPORE

**8–11 JANUARY, 2017** | DUBAI, UAE

PLAN NOW TO TAKE THE CCEP-I® CERTIFICATION EXAM AFTER YOU COMPLETE THIS INTENSIVE TRAINING

GET CERTIFIED
ENROLL NOW

**8,600+** COMPLIANCE PROFESSIONALS HOLD A COMPLIANCE CERTIFICATION BOARD (CCB)® CREDENTIAL

**CLE** APPROVED

CCEP-I® INTERNATIONAL
Certified Compliance & Ethics Professional

**REGISTER EARLY TO RESERVE YOUR PLACE**

LIMITED TO 75 FOR EACH ACADEMY

SCCE Academies. Training more than 3,500 compliance and ethics professionals around the world.

www.corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org

# ISACA Journal



## FEATURES



## PLUS



## Online-exclusive Features

Do not miss out on the *Journal*'s online-exclusive content. With new content weekly through feature articles and blogs, the *Journal* is more than a static print publication. Use your unique member login credentials to access these articles at *www.isaca.org/journal*.

**Online Features**
The following is a sample of the upcoming features planned for May and June 2016.

**Elements of an IS/IT Audit Strategy, Part 2**
Ed Gelbstein, Ph. D.

**Security Predictions 2016: A Data Analysis Approach**
Daniel Schatz, CISM, CCSK, CISSP, CSyP, CVSE, ISO27001 LA/LI, MCITP-EA

**The Interview as an Audit Tool During an IT Audit**
Henry Bottjer, CISA, CRISC

Discuss topics in the ISACA Knowledge Center: *www.isaca.org/knowledgecenter*
Follow ISACA on Twitter: *http://twitter.com/isacanews*; Hashtag: #ISACA
Join ISACA LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

The *ISACA® Journal* seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The *Journal's* noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

**Read more from these *Journal* authors...**

*Journal* authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA community.


ISACA®
*Trust in, and value from, information systems*

3701 Algonquin Road,
Suite 1010
Rolling Meadows, Illinois
60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
*www.isaca.org*

# THERE'S NO SHORTAGE OF CYBER SECURITY THREATS

## BUT THERE IS A **SHORTAGE OF IT SECURITY PROFESSIONALS**

## DO YOU HAVE WHAT IT TAKES TO BE PART OF THE **SOLUTION**?

**Get up-to-date security skills** with Capella University's Master's in Information Assurance and Security (MS-IAS).

Specializations include Digital Forensics, Network Defense, and Health Care Security.

Along the way to your MS-IAS, earn up to 3 NSA focus area digital badges showcasing your mastery of skills in specific cybersecurity areas.

Plus, the knowledge you gained for your CISSP®, CEH®, or CNDA® certifications can help you earn credit toward your MS-IAS, saving you time and money.

**ANSWER THE CALL.** START TODAY. **CAPELLA.EDU/ISACA** OR **1.866.933.5836**

See graduation rates, median student debt, and other information at www.capellaresults.com/outcomes.asp.

**ACCREDITATION:** Capella University is accredited by the Higher Learning Commission.
**HIGHER LEARNING COMMISSION:** https://www.hlcommission.org, 800.621.7440
**CAPELLA UNIVERSITY:** Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis MN 55402, 1.888.CAPELLA (227.3552)



Capella University

information security matters

# Chief Cyber Officer

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

A few columns back,[1] I used the term "chief cyber officer." I had not thought of a position by that name until the moment I wrote it, but the term has stuck with me. I did a search on it at the time I was writing and found nothing.[2] It has rattled around my brain long enough. I think the time has come for me to address the need for such a position.

## The Chief Information Security Officer and the Chief Cyber Officer

I can hear the rejoinder now: There is no need for a chief cyber officer because the chief information security officer (CISO) performs that function. Evidently Google thinks so as well. A search for "chief cyber officer" mostly brings up references to the CISO position. I maintain that there is a need for both, with, perhaps, a reporting relationship between them, with either a dotted or solid line. I see the chief cyber officer having a broader responsibility than information security as we have known it.

**Steven J. Ross,** CISA, CISSP, MBCP
Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersintl.com.*

This is not meant as an indictment of the CISO function or of CISOs and other information security professionals. We must remember that the threat of cyberattacks is still new. The term "cybersecurity" (or "cyber security," if you prefer) did not enter the English language until early in this decade. The fact of cyberattacks is more important than the term. I cannot find references to deliberate, targeted, malicious attacks on information systems (my definition of cybersecurity) other than international espionage prior to the mid-2000s.[3] But information security professionals were hard at work well before then. The issues of the time were—and still are—viruses and worms, fraud, insider misuse, data leakage, encryption, and private key infrastructure, digital signatures and business continuity planning. These concerns may not have the sexiness of confronting foreign governments, terrorists and criminals, but they are still essential to the safe use of organizational and personal information resources. The mandate of a chief cyber officer would incorporate some aspects of information security, but would go beyond it.

Central to the differentiation of roles is my contention that information systems are not vulnerable to cyberattacks simply because they are poorly protected, but because they are poorly constructed.[4] Therefore, it follows that combatting these attacks goes beyond the purview of an information security department. What would a chief cyber officer do that a CISO is not doing?

## Upgrading System Architectures

The underlying problem that enables attackers to get into information systems is that, historically, systems have "a hard crunchy outside and a soft chewy center."[5] If someone can penetrate the external barriers of firewalls and virus filters, he/she is free to roam around an organization's IT environment. Thus, the weakest point in a network defines the penetrability of the environment as a whole.

Solving this problem requires not only patching the holes, but reconstructing the entirety of an organization's systems architecture, not solely its

security architecture. This is a time-consuming, difficult and extremely expensive undertaking that must be carried out thoughtfully and carefully. With cybersecurity as the rationale for rebuilding a system architecture, it requires the knowledge, authority, and budget of an executive with a broad range of architectural skills, overseeing systems administrators, network engineers and database administrators, as well as information security specialists.

Re-architecting an IT environment is not going to be accomplished quickly. It must be rolled out over a period of years, perhaps many years. What is required at the outset is a reference architecture so that as systems are upgraded and changed, they can be accommodated to the intended to-be environment. This is a systems engineering mission, not one of information security alone.

## Decision Making

There is, perhaps, no more crucial function for a chief cyber officer than recognizing that an attack is underway and initiating a response. It means that preventive systems have been breached and detective mechanisms have been activated, preferably at the time of the attack. This is not always the case. The Ponemon Institute reports, "Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify."[6]

Chief information officers (CIOs) often wait for business leadership to authorize the closure of a data center or a network. Cyberattacks demand rapid decisions. Therefore, a chief cyber officer must be empowered to make those decisions and be inoculated by the board of directors (BoD) from criticism by business managers.

## Preparedness and Recovery

While a cyberattack is, *ipso facto*, a security incident, the response to it has to do with restoring servers and databases, not information security systems. These are involved only to the extent that any flaws that allowed an attack to proceed must be eradicated. The people who carry out the actual identification and removal of malware and the restoration of systems and data are those responsible for the systems and data—application developers, system administrators and database administrators (DBAs).

When and if an attack occurs, the response must be swift and disciplined. This requires ongoing training and drilling of and by the technical staff. A chief cyber officer would provide the leadership and oversight for what I call a CyberCERT,[7] which would be deployed at the first notice of a potential cyberattack. Many alarms will be false ones, so the expertise of the CyberCERT would be essential to identify a real attack and then move nimbly to respond to it.

**"A chief cyber officer would provide the leadership and oversight for what I call a CyberCERT, which would be deployed at the first notice of a potential cyberattack."**

## Coordination

I see the chief cyber officer as an executive who draws on skills from many functions. These would surely include technical and information security specialties, but also those of legal, communications, training, physical security and risk management. The chief cyber officer would be the main channel between the BoD, the top tier of management and all the aforementioned specialists insofar as an organization's cybersecurity defenses are concerned. Externally, the chief cyber officer would represent a company or agency in dealings with police and security agencies, as well as with the media, customers and shareholders, when issues of cybersecurity arise.

## Enjoying this article?

- **Learn more about, discuss and collaborate on career management and cybersecurity in the Knowledge Center.** *www.isaca.org/knowledgecenter*

## Politics

This will not be an easy job to fill or to execute. The effectiveness of a chief cyber officer position is dependent on the credibility of the threat of cyberattacks within an organization. Without that, there is no way for a chief cyber officer to demonstrate that he/she is actually achieving anything. Almost every day of the year there will be no cyberattacks, so there is no way to show progress, much less success. This has been a conundrum for CISOs for years, so it should not come as a surprise.

The relationship between the chief cyber officer and CISO could be fraught with jealousy, rivalry and internecine politics. It may be resolved, as I stated previously, by having one report to the other. However, that sets up a competition for limited funds allocated to information security that would only create its own political strife.

The potential for political infighting might be eliminated (or at least lessened) by appointing the person who is the CISO as the chief cyber officer. If such a position is established, moving the CISO into it is a logical career move. But this is predicated on the CISO having the skills and experience for the broader role as described. Many CISOs I know are well suited to be a chief cyber officer, but some do not have the verbal and interpersonal skills that would be essential for success in a coordinating role.

I do believe that there are CISOs and CIOs who are *de facto* chief cyber officers today. From the perspective of corporate governance, it is time to recognize that fact and set apart the cybersecurity function from that of building and implementing information security measures and running IT departments.

## Endnotes

1 Ross, S.; "Cyber/Privacy," *ISACA® Journal*, vol. 1, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

2 As I write this, Google tells me that there are a few references to chief cybersecurity officer, which I will grant is pretty close to the same thing. But four references doth not a trend make.

3 The Merriam-Webster online dictionary cites the first use of the term in 1994, without attribution. I do not believe the term was in general use until around 2010. *www.merriam-webster.com/dictionary/cybersecurity*. The events of the mid-2000s that I refer to were attacks on the systems of the Estonian government and the theft of 45.7 million payment cards used by customers of US retailer TJX. See *NATO Review Magazine*, 2013, *www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm,* and Franscella, Joe; "Cybersecurity vs. Cyber Security: When, Why and How to Use the Term," Infosec Island, 17 July 2013, *www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html*

4 Ross, S.; "Microwave Software," *ISACA® Journal*, vol.1, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*

5 Not original to, but quoted from Kindervag, John; "Developing a Framework to Improve Critical Infrastructure Cybersecurity," National Institute of Science and Technology, USA, 8 April 2013, p. 3

6 IBM, Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," 27 May 2015, p. 3, *www-03.ibm.com/security/data-breach/*

7 Ross, S.; "CyberCERT," *ISACA® Journal*, vol. 5, 2014, *www.isaca.org/Journal/archives/2014/Volume-5/Pages/CyberCERT.aspx*

IS audit basics

# Elements of an IS/IT Audit Strategy, Part 1

The word "strategy" often means different things to different people. For this column, it would be pertinent to remember the story of the person who decides to walk the hills to reach a specific village without a global positioning system (GPS) device. He gets lost, but can still see the village in the distance. Encountering a shepherd, he asks the question, "How do I get to the village?" "Well," the shepherd replies, "I would not start from here."

This article regards an IS/IT strategy as the set of steps that will allow the chief audit executive (CAE) and the IS/IT auditors to define their starting point, identify their target state, and determine the processes and resources that will get them there. **Figure 1** provides an overview.

While the figure illustrates the sequence of events as they need to happen in practice, this discussion shall follow the reverse path, starting with the audience. The reasons for this are that senior management and the audit committee define—separately and independently—whether or not the audit strategy is approved and endorsed. They also approve the resources necessary to implement it. The opinion and agreement of the chief information officer (CIO)—the target auditee—would help in the implementation of the strategy, but if this is not forthcoming, it would be desirable to understand exactly why not. The role of the external auditors may or may not be relevant, depending on the nature of the organization and the exact role of these auditors.

Without appropriate approvals, the proposed strategy is no more than a wish list.

## The IS/IT Audit Strategy Deliverables

The CAE proposing a strategy is undoubtedly aware that IS/IT is only a part, however important, of the overall audit universe of the organization. Therefore, the proposed strategy should reflect how information systems, technologies and data management fit in with the overall risk-based approach to auditing.

**In April 2016, Ed Gelbstein was awarded the Michael Cangemi Best Article Award posthumously. The award recognizes individuals for major contributions in the field of IS audit, control and/or security publishing. ISACA congratulates Dr. Gelbstein's dear wife, Cora, who received the award on behalf of her husband.**

### Audit Priorities

These vary from organization to organization, depending on the organization's placement in the private or public sector, its listing in the stock exchange or private ownership, and the regulatory compliance framework in which it operates. Compliance with internal rules and regulations are also factors.

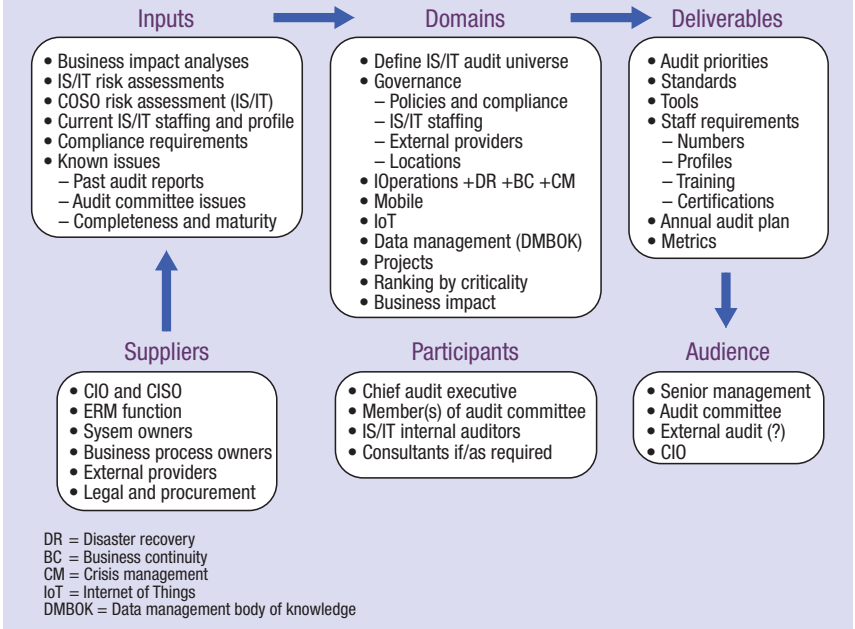
Other considerations include:

- Business activities and processes (operational, financial, legal, reputational, etc.) that have a potentially critical impact on the business
- The role of IS/IT in supporting them, indicating which have been recently audited
- Recommendations that have not been implemented and those that have been implemented, but may require being audited again

**Ed Gelbstein,** Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late 60s and early 70s, and managed projects of increasing size and complexity until the early 1990s. In the 90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi) retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Figure 1—Elements of an IS/IT Audit Strategy**




**Source:** Ed Gelbstein. Reprinted with permission.

### Audit Standards, Frameworks and Guidelines

Relevant audits standards frameworks and guidelines are updated or revised from time to time and the CAE should ensure the latest version is adopted and indicate any transition steps required to move from the previous version to the new version. For example, the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Enterprise Risk Management—Integrated Framework* was revised in May 2013 and, similarly, COBIT® 5 and its related documents have replaced COBIT® 4.1, Risk IT and Val IT. Transitioning from one version to the most recent is not a trivial task; it demands considerable effort and learning.

Internal auditors frequently consider the Institute of Internal Auditors (IIA) as the source of *de jure* standards and differentiate them from those used for IT and security. IS/IT auditors have several options to adopt; *de facto* standards, frameworks and guidelines are available from several sources, such as ISACA®[1] and the US National Institute of Standards and Technology (NIST). The strategy should indicate how these guidance documents complement each other and, in particular, how the proposed selection maps against the enterprise risk management (ERM) framework adopted by the business.

### Tools

In particular, computer assisted audit tools and techniques (CAATTs),[2] are becoming increasingly popular, in particular those that support several functions such as:

- Continuous monitoring/continuous auditing to enable auditors to monitor user activity, applications controls and business transactions
- Data analysis and tests
- Management of working papers (essentially a centralized database of past and current audit documents). Some may debate whether this is a CAATT. Products are also available to support the standardization of formats, thus increasing the consistency (and potentially the quality) of audit documentation.

Many commercially available products exist, but they are not addressed in this article.

As in the case of standards and frameworks, (often costly) tools need to be purchased, but they are of little value unless their users are well versed in their functionality and exploit these features during the execution of the audits. This implies a commitment to learning on the part of the IS/IT auditors and an effective approach to training.

### Staff Requirements

This would seem to be a simple issue to address (in theory). The IS/IT auditor is the right individual, but he/she must be knowledgeable, qualified and

experienced, and have the right soft skills.[3] The challenges for the CAE and the lead IS/IT auditor are to identify and justify a strategy that covers:

- **Auditor numbers**—This requires analyzing the strategy and the associated audit plans to determine the number of auditors needed to do the work to the required degree of quality across the critical part of the business. This calls for serious considerations. Many businesses that are too small to have an ERM function or an internal auditor depend on external intervention from their headquarters if they are part of a large business (for example, the country office of a multinational located elsewhere), auditors contracted by a qualified vendor company, or an independent traveling auditor. Other businesses and the not-for-profit sector may be unable to fund a suitably resourced audit function. Outsourcing this activity is seen as being more cost-effective than recruiting and training a team.
- **Auditor profiles**—This part of the strategy must consider several characteristics of the available auditors without infringing on their right to privacy. For example, it may be pertinent to evaluate the ages of the auditors for the purpose of thinking ahead about their probable retirement time frame or their ability to move to another job elsewhere (staff turnover is a good risk indicator). Age may also indicate their experience, which may be especially relevant to certain audits. This evaluation can support the strategy in defining the role of certifications and identifying any gaps between current knowledge and that required to apply changing frameworks and guidelines. The gap analysis should also include how to bridge the gaps (formal onsite training, face-to-face courses, self-paced computer-based training or on-the-job training).
- **Annual audit plan**—This deliverable states what will be audited in the next year with enough details on timing and resources to allow the target auditee to prepare.
- **Metrics**—For the strategy to be meaningful to those who must approve it and make the resources available to implement it, the measures of success[4] that will be used to evaluate the strategy must be described, highlighting the quantifiable metrics that will be used and reported.

## Conclusions

This article, which is the first of a two-part series, concentrates on what an audit strategy should deliver and to whom. This is the easy part. The challenges discussed in part 2 are in defining the continually changing and expanding IS/IT audit universe and ensuring that the focus remains on what is critical so that the audit is truly risk based.

Perhaps the hardest part is getting the full cooperation of those expected to supply information (represented by Inputs and Suppliers in **figure 1**). Few are likely to make the time to focus on this and there may be elements of organizational politics to overcome.

## Endnotes


1 ISACA, "Standards, Guidelines, Tools and Techniques," *ISACA® Journal*, vol. 3, 2016, *www.isaca.org/archives*

2 ISACA, Audit Tools and Techniques, *www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/Pages/Overview.aspx*

3 Gelbstein, E.; "The Soft Skill Challenge," *ISACA Journal*, vol. 3, 2015, *www.isaca.org/archives.* Gelbstein, E.; "Is There Such a Thing as a Bad Auditor, Part 1 and 2," *ISACA Journal*, vol. 1, 2016, *www.isaca.org/archives*

4 Gelbstein, E.; "Trust, but Verify," *ISACA® Journal*, vol 1, 2016, *www.isaca.org/journal/archives*




**Debbie Newman,** CISA
Is a senior global IT auditor with Abbott Laboratories. In this role, she focuses on critical information controls, specifically, testing the design and operating effectiveness of those information controls to verify compliance with professional standards.

**Q: How do you think the role of the IS auditor is changing or has changed? What would be your best piece of advice for IS auditors as they plan their career path and look at the future of IS auditing?**

A: The fundamental role of the IS auditor has not changed for many years with regard to the type of risk we try to address. IS auditors will be challenged in the future to address new areas of risk and move away from general computer controls that have long been effective in organizations. As risk is transferred to third-party vendors, IS auditors will be challenged to show how controls are effective when they are no longer being performed in-house.

**Q: How do you see the roles of IS audit, governance and compliance changing in the long term?**

A: In the next few years, IS audit, governance and compliance will move toward continuous auditing through the use of data analytics. Once a transaction hits an enterprise resource planning (ERP) system, users will be informed if it hits a certain threshold and causes suspicion. Instead of waiting until the next year when the population is reviewed by an auditor, key flags will already notify the system owners with potential areas of concern.

**Q: How have the certifications you have attained advanced or enhanced your career? What certifications do you look for when recruiting new members of your team?**

A: I obtained the Certified Information Systems Auditor® (CISA®) certification within my first year of working in public accounting. After obtaining the certification, I was able to show internal and external stakeholders that I knew the industry standard for IS audit.

I do not have certifications that I look for specifically when recruiting new members to my team; however, a technical certification shows me that an individual has taken the time to learn the industry's guidelines for best practices. It shows me they are dedicated to the profession outside of their normal business activities.

# the network

**Q: What would be your best piece of advice for IS auditors planning their career paths and looking at the future of IS auditing?**

A: Take lots of notes! I am constantly referring back to notes I wrote months and years ago. Sometimes they are technical items and other times it is a piece of advice from a colleague. You never know when you are going to need to refer to something from the past.

**Q: What has been your biggest workplace or career challenge and how did you face it?**

A: Learning to "work where your feet are." Audit professionals are constantly challenged by new work environments. I had to learn very quickly how to block out any outside distractions when working on trains, planes and in various conference rooms. Often, the places where we do our jobs may not be the most comfortable or conducive for being productive. I have found the best way to overcome the challenge of working in multiple locations is to set tasks based on where you will be working next. Sometimes, administrative tasks such as reporting travel expenses are best performed on a train, whereas documenting audit procedures is best performed on my couch.

## 1 What is the biggest security challenge that is being faced in 2016?

Identity and access management. We struggle with managing our own identities on a personal level with usernames, passwords and security questions to dozens of web sites. Organizations feel the same struggle when users have access to dozens of applications.

## 2 What are your three goals for 2016?

- Spend time with my family and friends
- Travel to at least six new countries
- Pass the CSX Cybersecurity Fundamental Exam

## 3 What is your favorite blog?

The Art of Advice by Justin Greis, *https://theartofadvice.com/*

## 4 What is on your desk right now?

Cup of coffee, pictures of my family and a calendar of "1,000 Places to See Before You Die"

## 5 Who are you following on Twitter?

I cannnot name all 631 of them. To name a few:

- @andylassner
- @oatmeal
- @sbellelauren
- @adam_newman
- @meritmusic

## 6 How has social media impacted you professionally?

It allows me to stay in touch with people I have met all over the world. I have been able to meet up with people who I have not seen in years because we connect and share our future travel plans via social media.

## 7 What is your number-one piece of advice for other IS audit professionals?

Keep in touch with everyone you meet! You never know when they will be part of your next project or team. The audit community is very small.

## 8 What is your favorite benefit of your ISACA® membership?

Access to publications and training materials through the online bookstore

## 9 What do you do when you are not at work?

- Try out new recipes and cooking techniques
- Travel to see family and friends

# Mobile Payments as a Security Control?

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Ask any merchant and he/she will tell you that accepting credit card payments comes with its own set of security challenges. Not only are there the (fairly prescriptive) requirements of the Payment Card Industry Data Security Standard (PCI DSS) to worry about, but being a security professional in a merchant context comes with a host of other things to cause concern as well. This includes staying ahead of potential fraudulent transactions, keeping tabs on where cardholder data are stored and the paths the data traverse inside a merchant's environment, ensuring the appropriate delineation between the cardholder data environment (CDE) and other environments, evaluating the security and compliance status of service providers, and numerous other issues.

The point is, payments can be challenging from a security point of view. Since no one has an unlimited budget, the onus is on security practitioners to find creative ways to address those challenges in a budget-conscious and efficiency-focused way. Being creative in this context often means looking to sometimes seemingly unorthodox ways to squeeze every drop of utility out of the opportunities that present themselves to advance security interests while ensuring those opportunities remain minimally impactful to business operations.

Believe it or not, mobile payment acceptance can be one such avenue. By understanding how mobile payments work under the hood—and looking for creative ways to turn that into an advantage from a security point of view—stakeholders can potentially take a few steps to move their security programs forward while, at the same time, providing a valuable service to customers.

**Robert Clyde,** CISM
Is managing director of Clyde Consulting LLC (USA). He also serves as a director on the boards of White Cloud Security (trusted app list enforcement); TZ Holdings (formerly Zimbra), a leader in community and collaboration software; and Xbridge Systems, a leader in data discovery software. He chairs a board-level ISACA® committee and has served as a member of ISACA's Strategic Advisory Council, Conference and Education Board, and the IT Governance Institute (ITGI) Advisory Panel. Previously, he was CEO of Adaptive Computing, which provides workload management software for some of the world's largest cloud, high performance computing (HPC) and big data environments. Prior to founding Clyde Consulting, he was chief technology officer at Symantec and a cofounder of Axent Technologies. Clyde is a frequent speaker at ISACA conferences and for the National Association of Corporate Directors (NACD). He also serves on the industry advisory council for the Management Information Systems Department of Utah State University (USA).

**Disponibile anche in italiano**
***www.isaca.org/currentissue***

## Why Mobile Payments?

Frankly, that statement might sound crazy to many practitioners. For example, ISACA's 2015 Mobile Payment Survey found that 87 percent of the 900 security practitioners surveyed expected to see an increase in mobile payment data breaches in the next year. About half (47 percent) indicated that mobile payments are not secure, and only 23 percent responded that mobile payments are secure in keeping personal information safe. So, clearly, it is an understatement to say that the profession views mobile payments with skepticism.

That said, it is worth considering the alternatives to mobile payments. Ponder for a moment the avenues for fraud and abuse available each and every time customers present their card to initiate a card-present transaction. Anytime the card is out of the cardholder's wallet, there exists the opportunity for it to be lost or stolen. There is the possibility of interception via the point of sale (i.e., via a skimmer), the opportunity for theft via the logical storage on the point of sale (POS) itself, the possibility of network sniffing between the POS and whatever system hands the payment details off to the payment processing back end, etc. At each and every step along that path, things could go wrong in a big way.

Now, compare that with a mobile payment scenario such as Android Pay, Samsung Pay or Apple Pay. Under those models, the primary account number (PAN) is protected via payment tokenization, transactions are authenticated using strong cryptography, and there are mechanisms in place to mitigate or even eliminate many of the fraud scenarios that one might encounter in a traditional card-present context. Moreover, there is a robust binding between

the cardholder and the payment transaction itself via the requirement for supplemental authentication (biometric or personal identification number [PIN]) before payment can be initiated.

No one is saying that mobile payments universally have more robust security properties in every use case that exists, rather it is simply suggested that there can be advantages in many situations relative to a traditional card-present transaction. Understanding that this is the case, mobile payment acceptance can then move from challenge to opportunity.

## Practical Risk Reduction

With this in mind, what are some ways that mobile payments can be leveraged to gain traction for security professionals in the field? The first area is to understand the security properties that mobile payments have and the possible benefits/drawbacks that come as a result as outlined here. To do this is not to suggest that one must read engineering specifications or the like, but it does behoove security professionals to understand the concepts at a high level since, ultimately, they will be making risk decisions about it. ISACA's recent white paper, *Is Mobile the Winner in Payment Security?*, outlines the business (and, yes, security) value propositions and describes some controls that can help security practitioners in the field mitigate some of the possible risk.

As the white paper explains in more detail, one of the key advantages of mobile payments using payment tokenization is that the PAN is not actually stored on the mobile device or transmitted to the merchant. Even if the merchant network is compromised, the PAN is not compromised, thus reducing the risk of theft or fraud.

This is a good starting point, but there is an additional way in which mobile payments can provide value to security programs even beyond this: Specifically, since the deployment of mobile payment acceptance requires an in-tandem refresh of the POSs in retail locations, that refresh can itself provide a useful opportunity to revisit those retail locations and simultaneously take a broader look at the security countermeasures in place (since, as any merchant can tell you, retail locations are often the point at which specific challenges occur).

Coupling a systematic revisiting of the security measures in place for retail locations—both as it pertains to the POS and to the location more generally—has a number of benefits. Keep in mind that to complete the documentation required under the PCI DSS program (a Report on Compliance [RoC] for larger merchants or a Self-Assessment Questionnaire [SAQ] for smaller ones), a subset of these locations would likely be under investigation potentially anyway. Specifically, since the retail locations involved in a payment transaction will almost always be part of the CDE, they are almost always included in an assessment. This means that the budget employed for the refresh of the POS could potentially serve two purposes by both upgrading that POS (and potentially mitigating certain areas of risk that already exist) as well as creating a broader opportunity to revisit other potential areas of concern at the retail locations themselves.

The rollout of mobile payment acceptance is certainly a challenge and carries with it an understandable uneasiness as the technology itself is relatively new. However, it does also present an opportunity for savvy professionals who know what to look for and can—like judo experts—turn the situation to their advantage.

**Enjoying this article?**

- **Learn more about, discuss and collaborate on mobile computing in the Knowledge Center.** *www.isaca.org/topic-mobile-computing*

# Mobile App Security Audit Framework

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

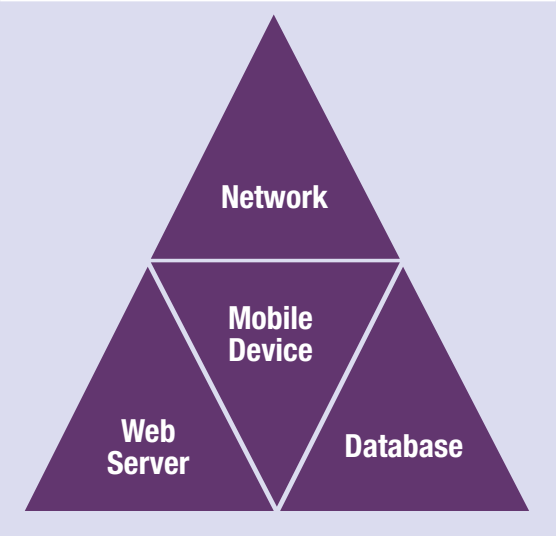
On 3 April 1973, Martin Cooper, a Motorola researcher and executive, made the first mobile call from a phone weighing a little over 1kg. Fast-forward to 2016. The average mobile phone is much lighter and faster than the 1973 version, it offers more functionality and it contains more computing power than the earliest personal computers. It seems clear that mobile technology is here to stay, as increasing numbers of consumers and enterprises alike adopt its convenience, speed and benefits. "As the number of people who own and use cell phones continues to grow, so does the use of smartphones. 91% of the US adult population currently owns a cell phone and of that 91%, 61% are smartphones."[1] With such technological change, especially at the enterprise level, IT audit and security professionals must adapt to the changing threat landscape created by mobile applications (apps) by getting ahead of the risk by putting proper controls in place and testing mobile apps from conception to release.

In order for the proper controls for mobile apps to be developed and tested, one must first dissect the layers of risk. As illustrated in **figure 1**, there can be multitudes of layers, but the basic risk segments can be divided into four main mobile app security categories:

- Mobile devices
- Mobile networks
- Mobile app web servers
- Mobile app databases

**Mohammed J. Khan,** CISA, CRISC, CIPM
Is a global audit manager at Baxter, a global medical device company. He works with the chief audit executive, chief information security officer and chief privacy officers. He has spearheaded multinational global audits in several areas, including enterprise resource planning systems, global data centers, third-party reviews, process reengineering and improvement, global privacy assessments (European Union and the United States), and cybersecurity initiatives in several markets over the past five years. Most recently, he has taken on further expertise in the area of medical device cybersecurity. Khan has previously worked as a senior assurance and advisory consultant for Ernst & Young and as a business systems analyst for Motorola.

**Figure 1—Four Segments of Mobile Apps Security Risk**




**Source:** Mohammed Khan. Reprinted with permission.

## Building a Framework at the Consumer and Enterprise Levels

Enterprise or consumer-only apps share the same types of risk and threats. However, some enterprise risk factors are unique in their own ways and, to address this risk, one has to assess the business value proposition for creating enterprise apps. According to one article, "Mobile devices dominate consumer use to the point that enterprises are seeing the value of integrating them into the workplace as well."[2] There are three desired benefits:

- **Efficiency**—The ability of the workforce to perform tasks typically performed on a client-server platform should be replicated to be performed the same way on a mobile app to achieve maximum mobility and benefit from the growing Internet of Things (IoT) capabilities.
- **Services**—Employees must be able to maximize the service they provide customers by being empowered to conduct enterprise-level activities in the same way they are accustomed to working with desktop applications. The app must provide the same type of support and data availability as is expected from the non-app enterprise-level services.

- **Customer satisfaction**—It is critical to provide customers the same enterprise-level satisfaction and meet the key performance indicators (KPIs) that formed part of the reason the customer signed up for the enterprise solution in the first place.

One of the challenges facing auditors is specifically assessing how to go about tackling risk factors in mobile apps. The layers illustrated in **figure 1** help the auditor dissect the threat areas. Also, there must be some basic controls in place for more complex controls to be addressed and implemented. Although the testing framework proposed in **figure 2** does not encapsulate all complementary controls, it focuses on the key controls required to have a basic maturity level around strengthening mobile apps security.

**Figure 2—Mobile Apps Audit Testing Framework**

| Threat Area | Control Topic | Control Test (Verify the Following) | Control Test | Risk Mitigated |
|---|---|---|---|---|
| Mobile device | Data storage | Data are stored securely to prevent malicious extraction from the app when data are at rest. | Encryption of the data at rest in the mobile device (app) is set to Advanced Encryption Standard (AES) 128, 192 or 256. | Data loss and disclosure |
| Mobile device | Data transmission | Mobile app data transmission is encrypted when data are not at rest (transferred). | Encryption of data is enforced for data in transit using Secure Sockets Layer (SSL) and strong security protocols such as:<br>• Web access—HTTPS vs. HTTP<br>• File transfer—FTPS, SFTP, SCP, WebDAV over HTTPS vs. FTP, RCP<br>• Security protocols—Transport Layer Security (TLS). | Data loss and disclosure |
| Mobile device | Reverse engineering of app code | App code is protected from modification from unauthorized intruders through use of binary protections. | Binary protections are standard protocol for app development life cycle and enforced by the development team at time of app coding and maintenance. | User experience compromise, unauthorized access, data loss |
| Mobile device | App access management and security | App is configured to limit access and configured appropriately for limited authorized use. | Mobile application management (MAM) is utilized to manage access and deployment of the app. Additionally, proper whitelists (approved) and blacklists (noncompliant) are maintained. Examples of MAM services include MobileIron, Airwatch and Apperian, providing a central online location for distribution and tracking purpose. | Unauthorized access and fraud |
| **Network** | Wireless connectivity | Encryption is enforced when Wi-Fi connection is activated. | Transmission of data utilizes, at a minimum, SSL or TLS—both cryptographic protocols for secure transmission of data. | Data loss and disclosure |
| **Network** | Session hijacking | Prevent hijacking of a session due to insecure connection protocol. | Connection protocols for the uniform resource locator (URL) via TLS are through HTTPS rather than HTTP to securely connect to a URL. | Data loss and disclosure, unauthorized access |

**Figure 2—Mobile Apps Audit Testing Framework *(cont.)***

| Threat Area | Control Topic | Control Test (Verify the Following) | Control Test | Risk Mitigated |
|---|---|---|---|---|
| Network | Domain Name System (DNS) spoofing | DNS is secured to avoid rerouting of data to another Internet Protocol (IP) address. | Proper packet filtering setup is built in to verify source address and blocking packets with conflicting source address. Utilization of TLS, Secure Shell (SSH) and HTTPS is enabled for secure communication protocol. | Data loss and disclosure, unauthorized access |
| Web server | Operations patch management | A process is in place to identify and apply critical system security patches and updates. | Processes exist for the deployment of system patches for all applicable systems. Processes exist for identifying new patches or for notification of new patches from vendors. The system is current with the latest patches prescribed from central IT. If any vulnerability scans have been performed, patches have been applied to address any identified issues. Missing patches are identified and compared against documented formal exceptions from security team. | Data loss and disclosure, unauthorized access |
| Web server | Access management | Roles and responsibilities for ownership have been established, documented and communicated. | All applicable web servers have been assigned both technical and business system owners, as required. The defined roles and responsibilities are adequate, especially for internal and third-party personnel. | Data loss and disclosure, unauthorized access |
| Web server | Brute-force attack | Management of denial-of-service (DoS) strategy encompasses proper programs to lock out unauthorized protocols. | Lock-out protocols are enabled for accounts with multiple incorrect password attempts. Utilization of CAPTCHA (program that distinguishes between humans and computers) is recommended to avoid DoS. | Unauthorized access and fraud, availability of app |
| Database | Privileged access | Elevated access to databases are properly secured utilizing best practices. | Access to database is limited to appropriate individuals, and proper access reviews and documented system accounts are kept on file. All default accounts and passwords are disabled by enforcing strict password controls. | Unauthorized access and fraud |
| Database | Structured Query Language (SQL) injection | Back-end database access is properly secured from vulnerabilities utilizing proper input validation techniques. | Input validation technique is in place; specifically defined rules for type and syntax against key business rules exist. | Unauthorized access and fraud |

**Figure 2—Mobile Apps Audit Testing Framework *(cont.)***

| Threat Area | Control Topic | Control Test (Verify the Following) | Control Test | Risk Mitigated |
|---|---|---|---|---|
| Database | Validation of app (client) input | Data coming from mobile apps have to be vetted prior to trusting it to pull or push data to the database layer. | Sanitization of app user data coming from the mobile app is properly protected through embedded logic checks within the application. Proper implementation of logic checks is enabled at the server side. | Unauthorized access and fraud |
| Database | App database services | Database server software is updated to current secure versions. | The database server is properly tested and hardened against malicious attack. Login forms have HTTPS required. SSL connections are mandatory. | Unauthorized access and fraud |
| App management | App deployment administration | App store updates are properly governed utilizing a life cycle management methodology. | A governance structure is in place for mobile app life cycle management, specifically, the release of mobile apps to the app store and modification of future releases. | Unauthorized access and fraud |
| App management | App deployment source code management | Source code management is properly assigned prior to release. | The app is signed using the enterprise account of the company's enterprise account certificate. | Unauthorized access and fraud |
| App management | Remote wiping of data | Ability for remote wipe of the device/app data exists to mitigate risk of lost or compromised devices. | Enterprise apps that are released to company employees or contractors using company-owned devices utilize a remote mobile management software, such as MobileIron, to facilitate remote wiping. | Data loss and disclosure, unauthorized access |

**Source:** Mohammed Khan. Reprinted with permission.

## Conclusion

It is imperative that IT auditors work with all teams within the organization responsible for the development of mobile apps—business, IT development, IT security, legal and compliance. Auditors must facilitate the process of policing the efforts of mobile app development and implementing a basic robust framework that determines a minimum amount of security controls that allow mobile apps to withstand the risk of operating in a vulnerable mobile environment. In addition to the basic auditing framework laid out in this article, it is recommended to use a penetration testing framework that applies to all mobile apps prior to their release. In addition, penetration testing must be performed as the mobile app is updated and newer technology is put in place to support the app. This reduces the risk of external and internal vulnerabilities that can result in the compromise of data.

## Endnotes


1 Collat School of Business, "The Future of Mobile Application," infographic, University of Alabama, Birmingham, USA, *http://businessdegrees.uab.edu/resources/infographics/the-future-of-mobile-application/*

2 Poole College of Management Enterprise Risk Management Initiative, "Managing Risks of the Mobile Enterprise," North Carolina State University, USA, 1 October 2012, *https://erm.ncsu.edu/library/article/manage-risks-mobile-enterprise*




# From Static Networks to Software-defined Networking

## An Evolution in Process

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

The networking industry is gradually transforming itself from a hardware-centric approach to a software-defined platform. Although the concept of software-defined networking (SDN) is still considered new and acceptance of it is at a very nascent stage, the life cycle and evolution of the personal computer indicate the benefits of such an architectural model and suggest the unstoppable direction in which the networking industry will eventually go.

SDN is largely considered to be at the conceptual stage. The implementation of SDN is dependent on the network strategy adopted by enterprises. SDN refers to all of the protocols and technologies that work in synchrony to create a global view of the network and provide a centralized, intelligence-based network service, delivery and control.

The Open Networking Foundation (ONF) is the organization that leads the effort of the promotion and adoption of SDN. It does this through open standards development. ONF mentions SDN as an emerging network architecture in which network control is made directly programmable and is decoupled from the forwarding plane.[1] This migration of control, from tightly bound in individual network devices to accessible computing devices, enables the underlying infrastructure to be separated for applications and network services, which allows administrators to manipulate networkwide traffic flow to meet the changing needs of today's business-driven networks.

**Nikesh Dubey,** CISA, CISM, CRISC, CCISO, CISSP
Is a cybersecurity specialist and governance, risk management and compliance (GRC) expert. He has a wide range of consulting experience in the fields of IS audit, information security and GRC. Working on different continents has given him an opportunity to look closely at the core issues, drivers, expectations and challenges of various enterprises. His previous *ISACA® Journal* article, "Corporate Responsibility—Retaining Top Management Commitment," discussed an innovative way to retain and improve management commitment levels, which is essential for the success of any program. He is currently associated with AGC Networks and can be reached at *nikesh.dubey@agcnetworks.com* or *nikesh.dubey@gmail.com.*

### The Challenge

The advent of new technologies, e.g., mobile devices, server and content virtualization, and cloud services, are among the key forces driving the networking industry today. These new technologies have forced the networking industry to take a fresh look at the traditional network architectures currently in use. Many typical networks are hierarchical in nature, built with layers of ethernet switches arranged in a tree-like structure. The key characteristic for traditional networks is that each device has a local control plane and a local data plane. Each device also has its own management planes, e.g., connecting to the device through Telnet, a simple, early network protocol that allows users on one computer to log into another computer that is on the same network.

The process of establishing the network topology using a control plane that runs locally is complex. This complexity results from no single device knowing the entire network. To manage each device, each device must be connected to its data plane individually to make configuration changes or updates, which is not an intelligent approach. The control plane is where the forwarding and routing decisions are made, while the data plane is where the commands of the control plane are executed. This traditional design did meet the needs of a time when client-server computing was dominant. However, such a basic architecture is not well equipped to meet the dynamic computing and storage needs of today's enterprise data centers and evolving technical landscapes due to changing business needs. Drawbacks of traditional networks include their static nature in contrast to the dynamic nature of today's server requirements. The complexities of today's networks make it difficult for IT to apply a consistent set of access. Hence, the traditional policies leave organizations vulnerable to security breaches and regulatory or noncompliance issues. Furthermore, networks must also grow to meet the needs of hundreds or thousands of newly added devices with different performance and service needs. The inability to scale up to meet these demands is a major limitation of traditional static networks. It is also understood that the lack of a standard in this area and

open interfaces often limit the capability of network operators to customize the network to their specific individual environments because they are hindered by the vendors' control of the equipment.

## The Genesis of SDN

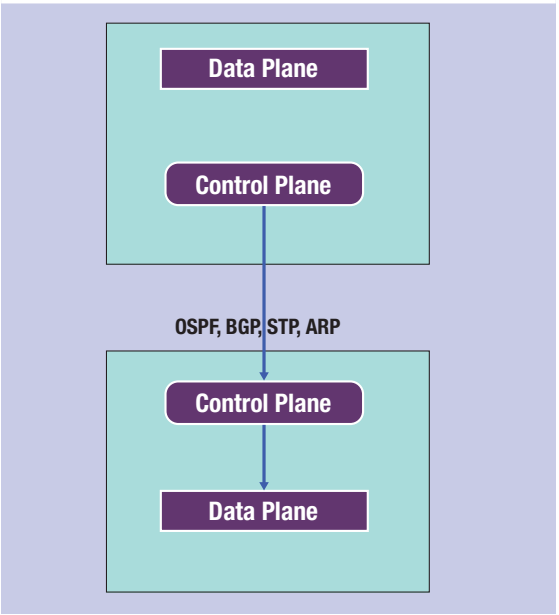
These disconnects between the increasing network industry requirements to support business and the existing static nature of traditional network capabilities have given birth to the concept of SDN. The basis of SDN is the concept of virtualization, which, in its most simplistic form, allows software to run separately from the underlying hardware. Virtualization has made cloud computing a reality today. There are several benefits of virtualization.

Virtualization allows data centers to quickly and dynamically provision IT resources exactly where they are needed. However, to keep up with the speed and complexity of split-second processing, there is a need for the network to also adapt, becoming more flexible and automatically responsive. The idea of virtualization can be applied to the network as well, separating the function of traffic control from the underlying network hardware plane into a centralized network-based intelligence control entity resulting in SDN. Thus, SDN is the natural next step in the evolutionary process of network architecture used today. The networking industry will gradually see a major shift in paradigm from a static, hardware-centric model to an evolving, software-defined model.

## A New Approach to Building Networks

Most networks deployed in today's environments require a great deal of manual administration. This is because traditional networks had the device-driven control plane interacting with the device-driven data plane (see **figure 1**), using protocols such as Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Address Resolution Protocol (ARP) and Spanning Tree Protocol (STP), and this was a limitation both from a technical and management perspective. The limitation arises because to configure and manage such traditional networks, the administrator needs to log into every device for intervention and manage the out-of-box capabilities driven by hardware appliances, which require configuration changes, making it tedious and resource intensive.

**Figure 1—Legacy/Traditional Networks**

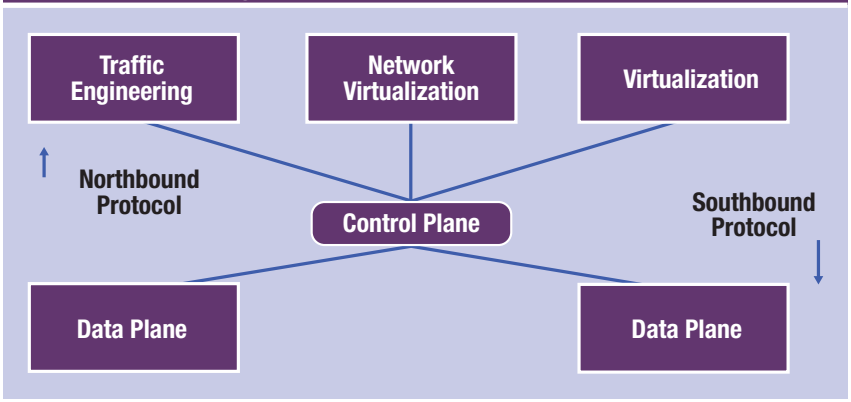



**Source:** Nikesh Dubey. Reprinted with permission.

However, the growing number of technologies using virtualization, cloud and mobility create more challenging and demanding environments; networks must appropriately support and adapt to these environments and manage their demanding requests in real time. SDN does this by introducing an abstraction layer that logically separates the control and data planes, centralizing the network intelligence layer. It also abstracts the underlying network infrastructure from applications with the objective of dynamically responding to changing network demands using controllable packet/flow processing protocols. This helps the SDN architecture provide networks with the advantages of visualization, traffic engineering and network virtualization.

There are several approaches to implementing SDN, but this article focuses on the most common components and concepts.

**Figure 2—Basic SDN Architecture**



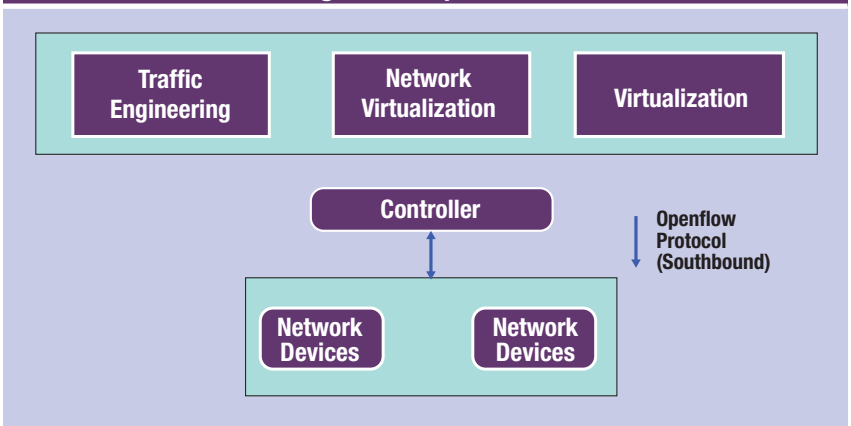

**Source:** Nikesh Dubey. Reprinted with permission.

## Basic SDN Architecture

At a basic level, SDN architecture consists of three layers: the application layer; the control layer or SDN controller; and the data, physical or infrastructural layer (**figure 2**). At the top is the application layer, which includes applications that deliver services, e.g., switch/network virtualization, firewalls and flow balancers. These are abstracted from the bottom layer, which is the underlying data or physical network layer.

In the middle is the control layer or SDN controller, the most important aspect of the SDN architecture. This layer removes the control plane from the physical plane and runs it as software while being integrated with the physical and virtual devices on the network, facilitating optimal network service management.

**Figure 3—Open SDN**




**Source:** Nikesh Dubey. Reprinted with permission.

## Open SDN

In Open SDN, the goal is to separate the control layer and data layer, creating a common language for programing network switches. The most common example of open SDN is OpenFlow, created by the ONF. SDN actually started with OpenFlow, which is a vendor-neutral communications interface defined in between the control and forwarding planes. OpenFlow internally provides an application program interface (API) or open interface to networking devices. It does not matter which operating system or vendor the networking device is using. With OpenFlow, there is an open interface to managing the device.

Typically, open-source tools are always a risk as they could be vulnerable. Lack of secure coding practices by novice and enthusiastic developers may allow vulnerabilities to creep into their code that may be exploited in the future. Organizations are weary of security issues when it comes to open-source tools. Opening the software's programmable interface to anyone who wants to come in and code makes the code vulnerable, devoid of quality coding practices and open to manipulations in the future. OpenFlow protocol is considered limited with insufficient functionality and scaling problems. **Figure 3** is the architecture of Open SDN.

## SDN Using APIs

APIs are an alternate way to provide the abstraction necessary for SDN and provide a highly programmable infrastructure. Programmable APIs provide a channel by which instructions can be sent to a device to program it. Programmers can read API documentation to understand the device and code the appropriate commands into their applications. As SDN has evolved, APIs are considered northbound or southbound, depending on the location where they function in the architecture (**figure 4**). APIs that reside on a controller and are used by applications to send instructions to the controller are called northbound because the communication takes place north of the controller. Examples of northbound APIs are RESTful and Java APIs.[2] These APIs allow the developer to manipulate flow tables and flow entries on networking devices (e.g., routers and switches) without talking to them

directly. The application developer is abstracted from the hardware and does not need to know the details and specific requirements of the switches, routers and other network devices.

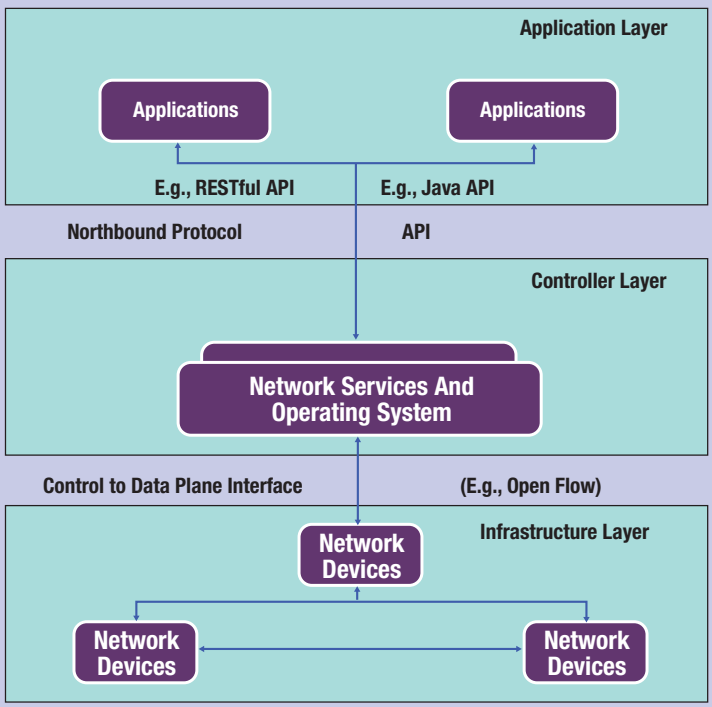
Southbound APIs reside on network devices, such as switches. These are used by the SDN controller to provision the network, with the communication taking place south of the controller. OpenFlow is a prominent southbound protocol. Another example of a southbound protocol is the Network Configuration Protocol (NETCONF).

## SDN Using Overlay

The advent of virtualization allowed for the possibility of the network overlay architectures to be created. Overlay networks run as separate virtual networks on top of the physical network infrastructure. When the concept of SDN was envisioned, the platform for leveraging the network overlay architecture already existed.

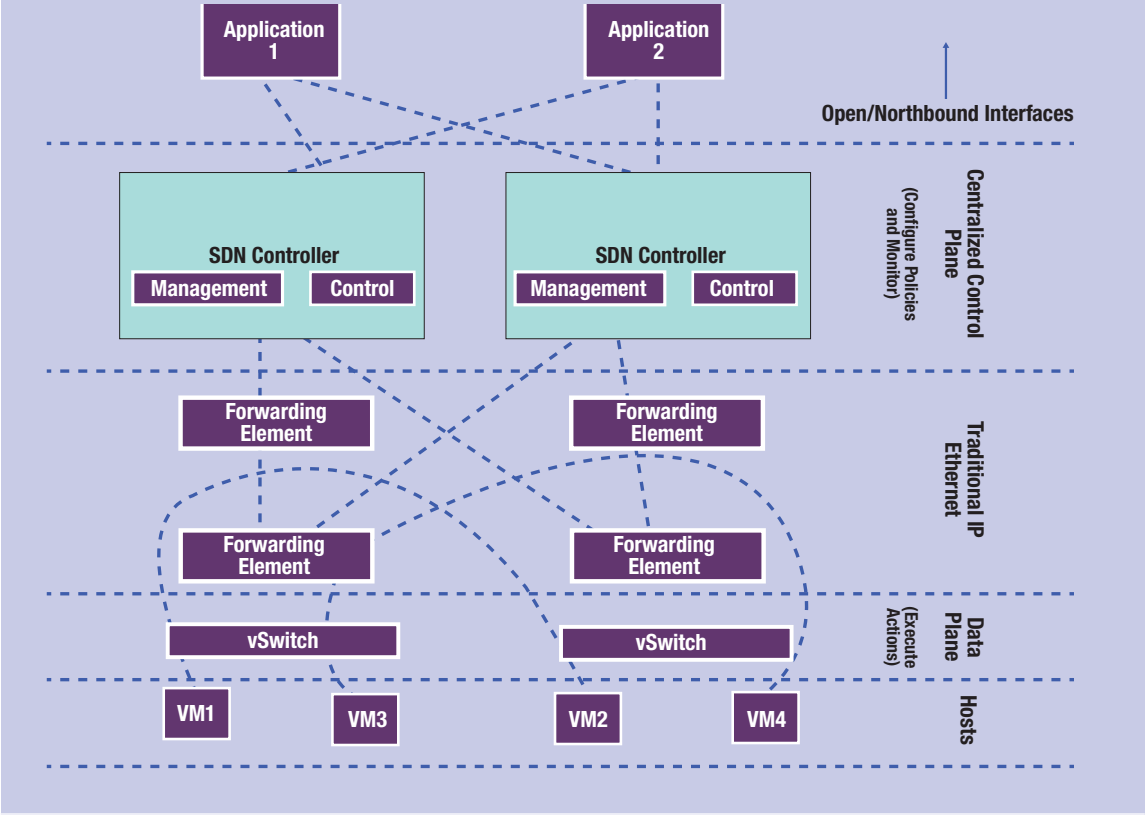
In SDN, using overlay nodes in the overlay network can be thought to be connected by virtual or logical links, each of which represents a path of its own so that there is an overlay of the virtual network and the existing physical one. This is the most popular model as it supports agility, which is key to networking solutions. In SDN overlay, the overlay implementation is built over the existing architecture to leverage a physical network that already exists. This suits organizations as they do not have to do anything other than add the new network over the existing one. The overlay is created using virtual switches inside hypervisors. A hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines. A host machine is a computer on which a hypervisor is running one or more virtual machines. Each virtual machine is called a guest machine. The controller communicates with the hypervisor's virtual switches. These set up tunnels that make use of the underlying physical network, but do not need to actually configure the hardware

**Figure 4—API-based SDN**




**Source:** Nikesh Dubey. Reprinted with permission.

Figure 5—Network Overlay SDN




**Source:** Nikesh Dubey. Reprinted with permission.

to send traffic to its destination. If agility is the key objective for the proposed network architecture, then overlay is a good choice to implement.

Virtualization technologies, e.g., Generic Network Virtualization Encapsulation (Geneve), Virtual Extensible LAN (VXLAN), Stateless Transport Tunneling (STT) and Network Virtualization Using Generic Routing Encapsulation (NVGRE), provide this solution by using network encapsulation. Big Switch Networks' Big Virtual Switch offers SDN overlay application using OpenFlow. **Figure 5** depicts a network overlay SDN architecture.[3]

## Advantages of SDN

There are numerous advantages of SDN. SDN increases network flexibility through holistic management of the network and enables rapid innovation. But why should organizations consider SDN, especially if it is still in the development stage and has not been widely adapted? The SDN model has the potential to make significant improvements to service request response times, security, reliability and scalability. It could also reduce costs by automating many processes that are currently done manually, which are resource intensive, slow and costly due to the use of restrictive commodity hardware. SDN offers a more efficient and flexible network that increases the speed of service delivery. It delivers cost savings on hardware and also offers the ability to test new protocols in hindsight.

## SDN Limitations and Challenges

Before looking at the limitations of SDN, it is important to understand the principal concept that drives SDN—virtualization. Virtualization adds overhead and network latency, which is an issue

for any operations that require fast response times from time-sensitive systems (e.g., financial systems or stock-related applications). It is also important to note that networking is static and not getting faster. Moreover, dependency on the Internet to do business is expanding traffic by a huge percentage, hence the demand to maintain or reduce existing response times would be a considerable challenge.[4] The need for faster speeds and the fundamental limitations of visualization, such as overhead and latency, may place limits on what SDN can practically achieve.

The adaptation of SDN will also be slow. This is because networks are considered the backbone of any infrastructure, and changing it is not easy. Unlike the adaptation of virtualization, which was more of an end-user change, SDN requires fundamental detailed planning as it impacts everything being serviced on the network. The centralized SDN controller also makes it vulnerable to become a single point of attack and failure.

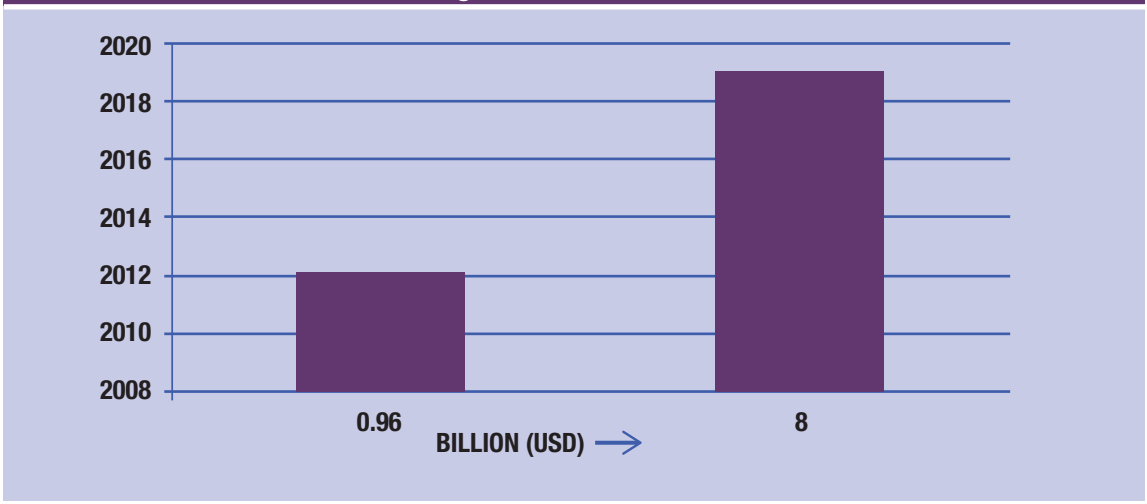
## Will SDN Really Catch On?

Although SDN promises to deliver benefits for the networking industry, the big questions are if anyone is using the concept productively and whether it will be the future direction of the network industry. There is an estimated rise in the SDN market worldwide from US $1 billion in 2014 to US $8 billion in 2018 (**figure 6**).[5] The SDN market includes network infrastructure, network virtualization, professional services, and network services and applications.

## Conclusion

Computers have evolved from a hardware-driven architecture to a software-defined module. In the 1970s and 1980s, the IT industry was primarily driven by hardware-centric devices that were limited in speed, size and network latency. The advancement in technology and its evolutionary process eventually guided it to a software-centric architecture, dramatically increasing speed and reducing size and cost, resulting in higher efficiency. The networking industry is undergoing the same transformations. The foundation of SDN is the concept of virtualization that has benefitted the IT industry in various ways. In principal, SDN promises to deliver a network that is enabled with network technology innovation and versatility while reducing complexity and administrative overhead and cost. It is important to identify the key pain points, drivers and use cases that SDN could address in an organization. If agility is the main priority, then organizations should deploy an SDN overlay solution. However, if there is a need to foster support for innovation in all three planes, then an

**Figure 6—SDN Growth**




**Source:** Nikesh Dubey. Reprinted with permission.

OpenFlow-based architecture takes precedence. If the focus is on programming APIs to better meet the specific needs of an organization through their applications, an API-based SDN is suitable.

In general, SDN offers agility by allowing external control and automation of the network, making it directly programmable. It offers management benefits by improving operational efficiencies by making network intelligence centralized in software-based controllers that maintain a full view of the network. Besides lowering the capital and operational costs, it is also important to note that SDN represents an entirely new way to manage network connectivity—one that is defined not by the vendors and equipment makers, but by those who use the network for their own business needs. SDN is intelligent and flexible enough to prioritize traffic; direct network resources to where they are needed most; and adapt, change and evolve over time to meet the business needs of today and address the challenges of the future.

## Endnotes


1 Open Networking Foundation, *Software-Defined Networking: The New Norm for Networks*, 13 April 2012, *https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf*

2 Bombal, David; "SDN and OpenFlow Overview—Open, API and Overlay based SDN," YouTube video, 28 October 2014, *https://www.youtube.com/watch?v=I-DcbQhFAQs*

3 Marschke, D.; "Is SDN Read for Prime Time or Junk Time?," APAC CIO Outlook, *www.apaccioutlook.com/ciospeaks/is-sdn-read-for-prime-time-or-junk-time-nwid-658.html*

4 O'Reilly, J.; "SDN Limitations," *Information Week*, 17 October 2014, *www.networkcomputing.com/networking/sdn-limitations/241820465*

5 Statica, "Software-defined Networking Market Size Worldwide in 2014 and 2018 (in Billion U.S. Dollars)," *www.statista.com/statistics/468636/global-sdn-market-size/*

# Benefits and the Security Risk of Software-defined Networking



**Disponibile anche in italiano**
***www.isaca.org/currentissue***

Traditionally, organizations increase their network bandwidth by focusing on buying more hardware. This approach does not always work, and it could be a costly mistake if the additional network resources are not fully utilized. As technology evolves, history finds a way to repeat itself. From the days of mainframe-based network protocols, such as Systems Network Architecture, the transition was made to the adoption of the universally accepted Transmission Control Protocol/Internet Protocol (IP) network protocol—a transition caused by the introduction of the personal computer (PC), which uses client-server computing technology. Now, with the disruptive and fast-paced changes from PCs to mobile devices, such as smart phones, which are enabled by virtualization and cloud-computing models, it looks as though the future of networking is increasingly going to rely on automated software. One might wonder about network evolution and how a modern network infrastructure will respond to the ever-changing demands of end users, commercial businesses and government regulators.

The growth in connected devices that could reside anywhere in the world has increased the complexity and difficulty of managing them and the related network traffic. There are very high costs associated with manually reconfiguring these devices for any required changes. Moreover, it is often difficult and sometimes almost impossible to reconfigure the traditional network in a timely manner to react to human errors and/or malicious events. Software-defined networking (SDN) makes use of virtualization to greatly expand network efficiency and, thus, simplifies the management of those consolidated resources and provides solutions for increased capacity without breaking the bank.[1]

## Benefits of SDN

What is SDN? Unlike traditional network design, SDN design is a paradigm shift that uses software-based controls to simplify the execution of policies with a centralized controller. It separates the data and control functions of networking devices, such as routers and switches, with a well-defined application programming interface.[2]

SDN architecture is logically separated into three planes: the application plane, the control plane and the data plane. The application plane incorporates SDN applications, which communicate the network requirements to the SDN controller. In turn, the software-based SDN controller interprets these requirements and executes the actual network policy from the control plane, which determines how data should flow from network devices. The SDN controller is the core of the SDN architecture, handling all complex functions and translating requirements into specific low-level rules. Finally, the data plane contains network devices, e.g., routers and switches, which execute the data flow once given permissions from the SDN controller. In essence, SDN decouples the network control and forwarding functions, enabling the network protocol to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.[3]

Since SDN uses a centralized controller with software applications, one of the biggest benefits of implementing SDN is its flexibility. Because the SDN controller assumes most complex functions (e.g., managing network intelligence and monitoring the network behavior in real time), the network

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Tony Wang**
Is the director of Williams Adley's IT risk management practice. He has more than 15 years of experience in evaluating internal controls, information systems and software development. Prior to joining Williams Adley, Wang held various management positions at BDO USA, Ernst & Young and Lockheed Martin, where he served clients in various industries, with a strong focus on government, health care, manufacturing, technology, nonprofit and financial services. His areas of specialty include engineering process auditing, integrated financial auditing, information assurance, IT security auditing, software development life cycle assessment, and systems integration and assessment. In addition to client responsibilities, Wang has spent a significant amount of time working on business development, campus recruiting, counseling, and developing and conducting training for IT auditors.

A centralized controller provides flexibility, programmability and a high return on investment (ROI) with its simplified network design.

devices just need to accept orders from the SDN controller. This eliminates the need for the network devices to understand how to execute data flow based on different communication protocols from various vendors. As a result, this gives network administrators great flexibility to configure, manage, secure and optimize network devices.[4]

> **"As companies adopt cloud technology, SDN will be able to simplify the overall network design by leveraging virtualization to automate network management operations."**

Furthermore, since the SDN controller is the brain of the SDN architecture, it is much easier to modify software programs/applications than manually reconfigure every single network device. This benefit alleviates the need for enterprises to purchase additional expensive network devices to meet ever-changing business needs. Therefore, SDN becomes a very cost-effective solution. In fact, SDN is designed to eliminate the dependence on the vendor locked-in network approach (i.e., vendors have their own proprietary management console and set of commands), which frees the enterprise to drive innovation and enhance network interoperability. As a result, it will greatly increase the ROI.

A majority of traditional network is managed using management consoles with a command-line interface that requires a lot of manual effort from network administrators.[5] As companies adopt cloud technology, SDN will be able to simplify the overall network design by leveraging virtualization to automate network management operations.

## The Security Risk of SDN

Many security issues related to the traditional network architecture also apply to the SDN architecture. Unfortunately, the new features that provide great flexibility, real-time programmability and simplified controls through the centralized SDN controller also introduce new security challenges. In fact, SDN is exposed to various sources of security risk from its network architecture design perspective, which includes the control plane, application plane and data plane layers.

One of the most significant security risk factors is the possibility of a compromised SDN controller attack at the control plane layer. Due to the centralization design of the SDN, the SDN controller becomes the brain of the SDN architecture. Attackers can focus on compromising the SDN controller in an attempt to manipulate the entire network.[6] If the attacker successfully gains access, the compromised SDN controller can be used to direct the network devices it controls (e.g., switches) to drop all incoming traffic or launch serious attacks against other targets, such as sending useless traffic to a victim to deplete its resources.[7] To mitigate this security risk, it is critical to harden the operating system that hosts the SDN controller and prevent unauthorized access to the SDN controller. Furthermore, the control plane layer is susceptible to a distributed denial-of-service (DDoS) attack. SDN switches may cause the SDN controller to be flooded with many queries that may potentially cause a delay or drop of queries. One possible defense against a DDoS attack is to implement multiple physical SDN controllers

If attackers compromise the SDN controller, they can hack the SDN applications to manipulate security applications to reprogram the network traffic flow through the SDN controller.

instead of just one. When switches are connected to multiple SDN controllers, one of these controllers can act as the master of the switches. When this master controller needs to process a high load of queries, it can direct the load to other lightly loaded controllers to be the master for some of its assigned switches. This keeps the load balanced among the SDN controllers, which mitigates DDoS attacks.

At the data plane layer, switches are vulnerable to denial-of-service (DoS) attacks as well. A malicious user can flood the switches with large payloads, causing legitimate packets to be dropped when a switch's buffering capability is exceeded. There are many ways to address this attack, including proactive rule caching, rule aggregation and decreasing the switch-to-SDN-controller communication delay. Also, increasing the switch's buffering capability can mitigate the risk of a DoS attack.[8]

Communicating messages between the control plane layer and the data plane layer is subject to man-in-the-middle attacks. The attacker can potentially modify rules sent from the SDN controller to switches to take control of the switches. One of the most effective solutions to such attacks is to encrypt the messages with the use of digital signatures for securing and proofing the integrity and authenticity of the messages.

The real-time programmability is also open to serious vulnerability at the application plane layer. Specifically, if the attacker can hack the SDN security applications, it can manipulate the network traffic flow through the SDN controller. If the SDN applications are compromised, the whole network is, too.[9] To effectively mitigate such security risk, it is critical that security coding practices be enforced with comprehensive change management and integrity check processes as part of the software development life cycle.

## Conclusion

Server virtualization, mobility and cloud computing are becoming the new norm to meet changing business needs. As these technologies evolve, the traditional network architecture is starting to fall short of meeting the significant network demands. The SDN architecture provides a virtualized network that transforms today's network into flexible and programmable platforms. The future of networking will rely more and more on software, and SDN, in turn, will become the new norm for networks. On the other hand, there is critical security risk that needs to be addressed regarding the SDN controller and applications before the SDN can be securely deployed.

## Endnotes


1 Underdahl, B.; G. Kinghorn; *Software Defined Networking for Dummies*, John Wiley & Sons, USA, 2015

2 Stallings, W.; "Software-Defined Networks and OpenFlow," *The Internet Protocol Journal*, vol. 16, no. 1, March 2013, p. 2-14

3 Open Networking Foundation, *https://www.opennetworking.org/sdn-resources/sdn-definition*

4 Open Networking Foundation, *Software-Defined Networking: The New Norm for Networks*, 13 April 2012, *https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf*

5 Kim, H.; N. Feamster; "Improving Network Management With Software Defined Networking," *IEEE Communications Magazine*, vol. 51, iss. 2, February 2013, p. 114-119

6 Open Networking Foundation, *Principles and Practices for Securing Software-Defined Networks*, January 2015, *https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf*

7 Mehiar, D.; B. Hamdaoui; M. Guizani; A. Rayes; "Software-defined Networking Security: Pros and Cons," *IEEE Communications Magazine*, vol. 53, iss. 6, June 2015

8 Dabbagh, M.; B. Hamdaoui; M. Guizani; A. Rayes; "Software-Defined Networking Security: Pros and Cons," *IEEE Communications Magazine*, vol. 53, iss. 6, May 2015

9 Lim, A.; "Security Risks in SDN and Other New Software Issues," RSA Conference 2015, July 2015




# Inquiring Into Security Requirements of Remote Code Execution for IoT Devices

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

The Internet of Things (IoT) is an evolving concept and is described in various ways, one of the most common being "an infrastructure of interconnected objects, people, systems and information resources."[1] It is obvious to practitioners, however, that IoT is not a new concept. It is a new paradigm that is created and realized through the use of old concepts, methods and tools that have been around for many years in the world of IT and computing. Some of these concepts include remote function call and remote code execution.

From a security perspective, however, IoT exhibits new features and characteristics, such as the need to share additional types of data and operations. In contrast with older systems, IoT devices receive various types of inputs from other devices in the form of data and remote commands.[2, 3] IoT devices (e.g., smart locks or printers) are required to run a set of commands that are sent to them by remote entities, such as phones, on the same network or fetch utility libraries that are placed on scattered servers (e.g., JavaScript libraries). It is common for IoT devices to receive a set of machine instructions or commands for updates to the software that controls the physical device (e.g., firmware) or instructions to tell the device what exactly needs to be done. In technical terms, the devices can use well-known methods of remote procedure call, remote method invocation, dynamic class loading, and download of shared libraries and objects.

This article focuses on the security requirements around remote code execution, which means receiving and running code/commands from another system on the same network. In the case of IoT, this amounts to a device (the source of instructions) being able to control a connected "thing" from anywhere in the world. Used maliciously, remote code execution is a serious threat. It is sought after by hackers:  being able to control a machine to do anything. Think, for example, of a malicious person being able to remotely control connected cars, medical devices or power plant control systems.

The article investigates security requirements of traditional remote code execution techniques in light of threat modeling results and expounds on the sections of security compliance regulations that stipulate those requirements.

## Types and Scenarios of Remote Code Execution

Remote code execution is an umbrella term used for various types of code sharing in which an entity requests or receives some code and runs the code in its own environment. These are the common scenarios in which remote code execution occurs:

1. **Use of common utility libraries placed on a remote server (e.g., JavaScript libraries).** The functions are fetched from the server, but run on the client (e.g., the browser).[4]
2. **Dynamic loading of (compiled) classes.** An example is Java dynamic class loading, which involves loading the binary form of a class (from a file or network location) that has been previously compiled from the source code.[5]

**Farbod Hosseyndoust Foomany,** Ph.D.
Is a senior application security researcher (technical lead) at SD Elements/Security Compass. Foomany has been involved in various academic research and industry projects in the area of secure software development, secure design for enterprise applications, signal processing and evaluation of biometric verification systems. Foomany is currently involved in a project that aims to investigate and formulate the security requirements of the IoT systems.

**Ehsan Foroughi,** CISM, CISSP
Is the vice president of the SD Elements division at Security Compass. Foroughi is an application security expert with more than 10 years of management and technical experience in security research and an extensive product management, development and reverse-engineering background. Prior to joining Security Compass, he managed the vulnerability research subscription service for TELUS Security Labs (previously Assurent).

**Rohit Sethi**
Is a specialist in software security requirements. He has helped improve software security at some of the world's most security-sensitive organizations in financial services, software, e-commerce, health care, telecommunications and other industries. In his current role, Sethi manages the SD Elements team at Security Compass. Sethi has appeared as a security expert on television outlets such as Bloomberg, CNBC, FoxNews, CBC, CTV and BNN. Sethi has spoken at numerous industry conferences.

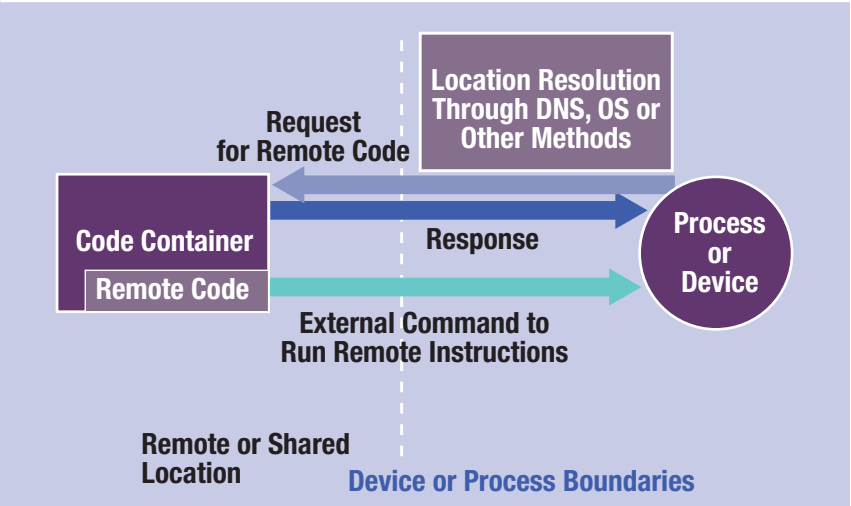
3. **Object serialization.**[6] Also known as marshaling, object serialization involves turning the object (structure, functions and attributes) into a new format (e.g., a byte stream) that could be easily transmitted and stored. Serialization and deserialization (sometimes called unserialization) is implemented in many languages such as Java[7] and C#.[8] JavaScript Object Notation (JSON) is built on the same concept; however, the goal of JSON is primarily data transfer rather than running remote code. Note that in this scenario, there is an instance of the class (an object with a set of properties) being transmitted. It is different from dynamic class loading in which the class (the binary) is loaded (usually only the structure, code and constants, and not a particular instance).
4. **Remote procedure calls (RPC) or remote method invocation (RMI).** There are numerous RPC protocols from older methods based on Common Object Request Broker Architecture (CORBA)[9] and Open Software Foundation (OSF) RPC to newer models of Java application programming interfaces (API) for Extensible Markup Language (XML)-based RPC (JAX-RPC) and JAX-WS (Java API for XML-based web services).[10] Calling web services such as Simple Object Access Protocol (SOAP) and Representational State Transfer (REST) web services[11] could also be considered a special case of RPC. However, note that if the code runs on the host (e.g., server) and only the result is passed to the requesting device, the process will not qualify as RPC.
5. **Device-specific operational commands.** This includes commands sent to a device or an embedded system to carry out a sequence of tasks. One example is commands in the form of HP Printer Job Language (PJL).[12] It is foreseeable that these types of proprietary and standard protocols will emerge and become widespread for numerous devices and applications as IoT matures.
6. **Device-specific control commands (including firmware update commands).** Firmware and basic input/output system (BIOS) update commands are very common for IoT devices, and the code may be received on the same channel as the device-specific commands (mentioned in scenario 5).There are also other standard and proprietary control commands that could be sent to devices according to IoT protocols.[13, 14]
7. **Executable code embedded in files.** Examples include code in the form of Postscript, ActiveX and Macros and embedded in files such as Microsoft Word, Microsoft Excel, PDF and Adobe Flash. The code is transmitted as part of the file and is executed at the destination. This concept is explained under the title of "mobile code" in American National Standards Institute (ANSI)/ International Society of Automation (ISA) 62443[15] and NIST 800-53[16] compliance regulations.

> **"Remote code execution is an umbrella term used for various types of code sharing in which an entity requests or receives some code and runs the code in its own environment."**

## Threat Modeling of Remote Code Execution

**Figure 1** displays a simple data flow diagram as recommended by the Open Web Application Security Project (OWASP) application threat modeling method.[17] The diagram shows the common elements of the described scenarios. The source of remote code is either a shared location (e.g., world-writeable locations on Android devices when dynamic class loading is used) or remote locations (e.g., a server on the Internet when a JavaScript library is loaded). A process or device (e.g., an IoT-embedded device) will eventually host and run the remote code. To determine the place of remote code and fetch data, a location resolution

**Figure 1—Flow Diagram of Typical Forms of Remote Code Execution**




**Source:** Farbod H. Foomany, Ehsan Foroughi and Rohit Sethi. Reprinted with permission.

service is utilized. For example, in the case of files in shared locations, the operating system can handle the requests and send them to the right resource. For Internet access, domain name servers translate the resource's address to an Internet Protocol (IP) address.

One important idea displayed in **figure 1** is that there are two conceivable flow directions. In some cases, the host/device initiates the request for the remote code. In others, the device receives the commands even though it has not necessarily initiated the request. For example, a printer may have a channel for receiving remote commands for performing various jobs.

Using spoofing identity, tampering with data, repudiation, information disclosure, denial-of-service (DoS), and the elevation of privilege (STRIDE) threat modeling technique, the security threats of remote code execution can be classified and summarized as follows:[18]

- **Spoofing identity**—Domain name system (DNS) spoofing can cause requests for one resource to be sent to another.[19] Other types of man-in-the-middle attacks can also facilitate misrepresentation of spoof code as original code. These threats are relevant to all seven types and scenarios of remote code execution described in the previous section.
- **Tampering with data**—Any form of data tampering in transit or at rest (e.g., tampering with data through man-in-the-middle attacks) can fall under this category. A specific form of this vulnerability occurs when the code is loaded from a shared or world-accessible location (e.g., universal serial bus [USB] storage connected to a PC or a world-writeable location on an Android SD card). Tampered data, if handled by typical remote code execution libraries (such as the deserialization libraries outlined in scenario 3 described earlier) without additional protection measures, can lead to malicious code execution similar to those reported for Apache Commons libraries.[20]
- **Information disclosure**—Any confidential data that are transmitted as part of an object (e.g., properties of a C# serialized object that constitute a person's health record) are vulnerable to unauthorized disclosure (especially for scenarios 3 and 4). Some of the serialization/deserialization or RPC steps are delegated to the libraries that do not use encrypted channels. Developers may be unaware of the underlying mechanisms used by those libraries (e.g., if a particular library uses an encrypted channel for remote procedure calls).
- **Denial-of-service**—The availability of a system that executes remote code can be threatened by malicious code. A simple form of attack may involve creating huge payloads and sending them to the system as code. This can occur in all seven scenarios. Even if the system carries out integrity checks, a large amount of data can hinder normal operation of the system and can eventually lead to denial of service. Additional threats to availability are overreliance on a remote resource and lacking fail-safe procedures when that resource is unavailable. Another major vulnerability emerges from the use of third-party libraries that lack DoS protection.

- **Elevation of privilege**—There are numerous situations in which insecure remote code execution can lead to elevation of privileges. For example, Android applications can dynamically load Java classes (scenario 2). The application that loads the classes passes all of its permissions to the class that it is running. The loaded class receives the application's permissions and privileges since the code is running in a new environment. Another example is if a device does not discriminate between various channels from which it receives commands (e.g., it does not separate its firmware update channel from the channel dedicated to its normal job), there is a risk of using permissions of one channel to perform unauthorized activities (scenarios 5 and 6).[21] Third-party libraries may also be a vulnerability.
- **Repudiation**—Any other vulnerabilities can create opportunity for repudiation.

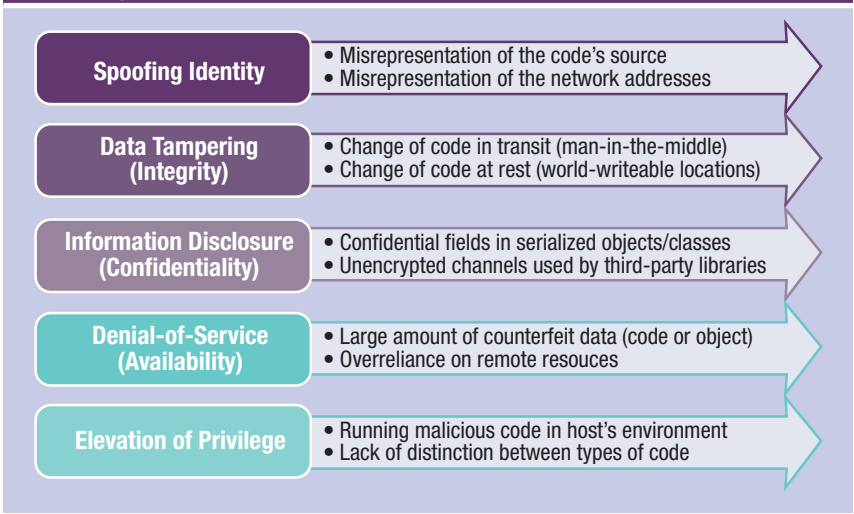
**Figure 2** depicts threats under various categories and also shows their relation to the security triad of confidentiality, integrity and availability. Based on all the identified threats and vulnerabilities, this article provides eight rules of remote code execution that mitigate these areas of security risk.

## A Prescriptive Approach to Securing Remote Code Execution

This section outlines a set of security requirements that mitigate the risk and threats relating to low-complexity IoT devices.

1. **Encrypt fields, obfuscate classes and use encrypted channels.** This requirement stems from the goal of confidentiality and the possibility of information disclosure. There are several ways to maintain the confidentiality of the data transmitted as part of objects or procedures by:
   - Encrypting individual fields (e.g., properties of the objects). Secure key management and distribution, especially for stand-alone devices, is an important undertaking in this case.
   - Obscuring or obfuscating code and objects. Binaries of compiled classes are easy to reverse engineer. By using decompilers, hackers can obtain the original code and any constants in the code. Obfuscation is not a panacea, but it adds a layer of defense, i.e., it should not be treated as the sole security measure. More information on this can be found in documents relating to the OWASP project on code reverse engineering.[22]
   - Communicating through an encrypted channel (e.g., Secure Sockets Layer [SSL]/Transport Layer Security [TLS] channels). It is important to keep an eye on the studies of SSL/TLS vulnerabilities and apply the result of those studies. There are several guidelines on the types of encrypted channels to use and what to avoid.[23] For example, SSL v2.0 and 3.0 are not secure, and SSL libraries need constant updates due to various vulnerabilities that are regularly discovered (e.g., Heartbleed, Browser Exploit Against SSL/TLS [BEAST], Factoring RSA Export Keys [FREAK] and Compression Ratio Info-leak Made Easy [CRIME] attack vector). An IoT device with no update capability will become insecure in no time. Implementing SSL/TLS on low-complexity

**Figure 2—Security Threats of Remote Code Execution**




**Source:** Farbod H. Foomany, Ehsan Foroughi and Rohit Sethi. Reprinted with permission.

devices is a challenge that may cause reliance on solutions a or b mentioned earlier instead of encrypting the entire stream of data, which is required by SSL/TLS.

2. **Check the size of payload.** Before anything else—even before checking the code signature—check the payload size and avoid dealing with large counterfeit lumps of data that are sent as part of a DoS attack.
3. **Sign the code or use protocol-specific authentication methods.** Signing the code and avoiding running any unsigned code is the single most important security measure. If using encrypted channels (e.g., TLS), validate the certificate and chain of trust. Signed code is not obviously secure code, but signature, at a minimum, manifests the integrity of code.[24]
4. **Do not run any part of the code before checking size and signature.** No constructor or overridden methods should be executed by the code or any third-party library before all security checks are performed. For example, a library contains a set class that handles serialized objects. The set class should not receive the external inputs before size/signature checking. It also should not run any part of the classes (e.g., constructors or overridden *readObject*() methods) before the object is validated.
5. **Sandbox the remote code execution process and memory.** Do not let the code run in a shared memory or storage space to which other processes have access and *vice versa* (especially the update commands). Sandboxing (direct access to other applications' storage and memory) does not protect against any of the vulnerabilities mentioned so far. However, since a lack of sandboxing can void other security measures (such as signature verification), sandboxing contributes to strengthening other defense mechanisms. In the case of a BIOS update, for example, researchers have shown that a buffer overflow can enable executing the unsigned portion of the update package.[25]
6. **Separate the channels of code transfer.** Make sure data on ordinary channels of data transfer (e.g., operational commands for a printer) cannot be used to carry out malicious remote code execution. Restrictions of update commands (e.g., signature requirements) should be different from the ones for ordinary commands.
7. **Verify that third-party libraries comply with the previous requirements.** Do not feed the libraries user data unless all the other checks have been carried out. For example, if the library is used before size-checking, an organization may make itself vulnerable to DoS attacks.
8. **Avoid overreliance on remote resource and have a fail-safe plan.** Devise an alternate plan for the situations that the remote resources become unavailable. If continuing the process may become impossible due to unavailability of those resources, design a fail-safe plan.

**Figure 3** displays a best practice for object serialization, in which the transmitted object is sealed (encrypted), then signed and then transferred. On the receiver side, the object is first size checked, then the signature is verified and finally decrypted.

## Relation to Major Security Compliance Regulations

ANSI/ISA 62443, under security requirement (SR) 2.4 (mobile code), instructs control systems to enforce usage restrictions on mobile code technologies that include: preventing the execution of mobile code, requiring proper authentication/authorization for origin of the code, restricting mobile code transfer and monitoring the use of mobile code.[26]

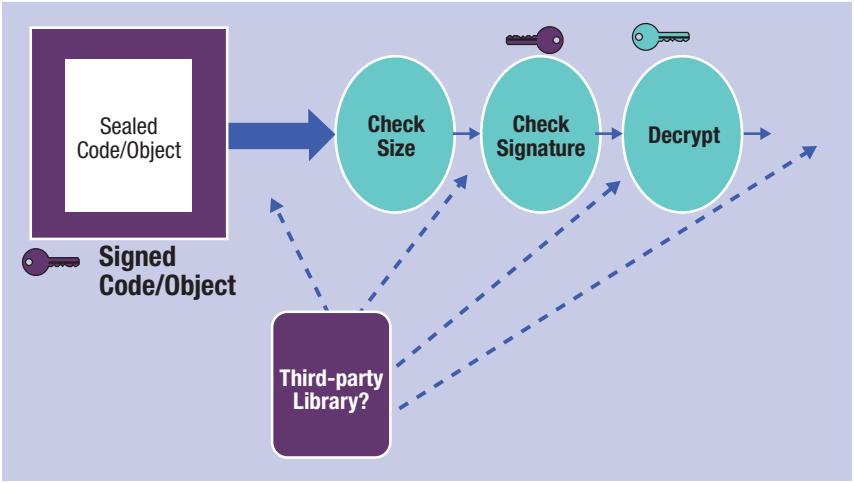
NIST 800-53r4 in the system and communications protection section (SC-18, mobile code), recommends execution of remote code in a confined environment.[27] In the section on system and information integrity, SI-7 (15), the standard stipulates code signing and verification.



The vulnerabilities described in this article are among the Common Weakness Enumeration (CWE)/SANS top 25 listed vulnerabilities: Download of code without integrity check (CWE-494) and inclusion of functionality from untrusted control sphere (CWE-829).[28]

The European Banking Authority's final guidelines on the security of Internet payments state that software delivered via the Internet needs to be digitally signed by the payment service provider.[29] In the Manufacturer Disclosure Statement for Medical Device Security (MDS2), the manufacturers are required to declare if the device protects transmission integrity (TXIG) and if there are any mechanisms to ensure that the installed code or update is manufacturer authorized (15-2).[30]

**Figure 3—A Secure Three-part Procedure for Object Serialization**




**Source:** Farbod H. Foomany, Ehsan Foroughi and Rohit Sethi. Reprinted with permission.

## Conclusion

Sending remote code in various forms to "things" and asking for instructions by those things, especially for device and firmware updates, is common and will become a more common practice in the IoT ecosystem. Since IoT devices have interaction with the physical world and, in many cases, those interactions are remotely controllable (whether in a thermostat or in the collision-prevention system of a connected car), the consequences of bypassing security controls are immense. Unsafe execution of remote code can lead to a bypass of safety controls and can cause physical harm to consumers of IoT products. Therefore, all security measures and relevant compliance regulation sections should be considered before any attempt to design security for IoT solutions.

## Endnotes

1 ISO/IEC, SWG 5 agreed on this definition of IoT in 2014: "An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react." ISO/IEC JTC 1, "Internet of Things (IoT) Preliminary Report," 2014

2 Athreya, A. P.; B. DeBruhl; P. Tague; "Designing for Self-configuration and Self-adaptation in the Internet of Things," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, 2013

3 Klauck, R.; M. Kirsche; "Chatty Things—Making the Internet of Things Readily Usable for the Masses With XMPP," 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom, 2012

4 Flanagan, D.; *JavaScript: The Definitive Guide: Activate Your Web Pages*, O'Reilly Media Inc., USA, 2011

5 Gosling, J.; *et al*.; "The Java Language Specification–Java SE 8 Edition," Oracle America, 2014

6 Deitel, P.; H. M. Deitel; *Java for Programmers, Second Edition*, Prentice Hall Professional, USA, 2011

7 *Ibid*.

8 Hericko, M.; *et al*.; "Object Serialization Analysis and Comparison in Java and .NET," *ACM Sigplan Notices*, vol. 38, iss. 8, August 2003, p. 44-54
9 Ben-Natan, R.; *Corba: A Guide to Common Object Request Broker Architecture*, McGraw-Hill Inc., USA, 1995
10 Fisher, M.; *et al.; Java EE and .NET Interoperability: Integration Strategies, Patterns, and Best Practices*, Prentice Hall Professional, USA, 2006
11 Richardson, L.; S. Ruby; *RESTful Web Services*, O'Reilly Media Inc., USA, 2007
12 Hewlett-Packard, Printer Job Language Technical Reference Manual, 2003, *www.hp.com*
13 *Op cit*, Athreya
14 *Op cit*, Klauck
15 ANSI/ISA, *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels*, USA, 2013
16 National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53r4, USA, 2013
17 Open Web Application Security Project (OWASP), "Application Threat Modeling," *https://www.owasp.org/index.php/Application_Threat_Modeling*
18 Shostack, A.; *Threat Modeling: Designing for Security*, John Wiley & Sons, USA, 2014
19 Shinder, D. L.; M. Cross; *Scene of the Cybercrime*, Syngress, USA, 2008
20 The Apache Software Foundation Blog, "Apache Commons Statement to Widespread Java Object De-serialisation Vulnerability," 10 November 2015, *https://blogs.apache.org/foundation/entry/apache_commons_statement_to_widespread*
21 Cui, A.; M. Costello; S. Stolfo; "When Firmware Modifications Attack: A Case Study of Embedded Exploitation," Presented at the NDSS symposium, 2013
22 See OWASP's Reverse Engineering and Code Modification Prevention Project, *https://www.owasp.org/index.php/OWASP_Reverse_Engineering_and_Code_Modification_Prevention_Project.*
23 Ristic, I.; "SSL/TLS Deployment Best Practices," 2013, *https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf*
24 *Op cit,* Cui
25 Wojtczuk, R.; A. Tereshkin; "Attacking Intel BIOS," BlackHat, Las Vegas, Nevada, USA, 30 July 2009
26 *Op cit*, ANSI/ISA
27 *Op cit*, NIST
28 Common Weakness Enumeration, "2011 CWE/SANS Top 25 Most Dangerous Software Errors," 2011, *http://cwe.mitre.org/top25/*
29 European Banking Authority, Final guidelines on the security of internet payments, 19 December 2014, *https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1*
30 HIMSS/NEMA, Manufacturer Disclosure Statement for Medical Device Security, 2013, *www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx*

# Data Science as a Tool for Cloud Security



## Cloud Generation Visibility, Detection and Protection

Sharing, collaboration and anywhere access are the prominent features of modern cloud applications. However, cloud security faces scalability challenges. In industries other than the cloud that are facing this same scalability problem, data science techniques have proven highly successful. Examples include web search, high-speed finance, high-volume image and video processing, and even large-scale defense systems. Recently, data science techniques have also been increasingly adopted in on-premises computer and network security applications. There is no doubt that data science can be used as a core technology to secure and strengthen cloud applications by implementing algorithms that can detect threats through large-scale data mining.

> **"The cornerstone of security is visibility."**

Using data science, it is possible to identify and extract critical information from a variety of structured or unstructured data by using techniques such as data mining, machine learning, statistics and natural language processing. The extracted information can be used to perform analytics and to gain insights into the target environment from which data are fetched. **Figure 1** highlights the different techniques that are used as building blocks of data science algorithms.

The cornerstone of security is visibility. For effective cloud application security, visibility means understanding:

- What cloud applications are used by employees
- What actions employees take
- What information employees create and distribute using the apps

Once this visibility is achieved, detection of malicious insiders and malware threats and protection of assets follows from having security systems that interoperate with cloud applications, which facilitates alerting, automatic prevention and remediation policies. Data science plays a significant role in attaining that visibility. Once visibility is achieved, there is the challenge of detecting threats. For cloud applications, the challenge is detecting abnormal user activities, hacking attempts or other threats that could potentially expose or destroy information stored on a cloud service. This necessitates a meaningful level of visibility that captures both user actions and the resources they access. For instance, is a user account being used to upload an abnormally large number of encrypted files (e.g., ransomware)? Is a user viewing an abnormally large amount of specific information (e.g., sales contacts) that he/she typically does not access? Fixed usage thresholds (e.g., upload limits) can correctly identify most aberrant behavior but are likely to result in costly false-positive alerts or a significant number of missed detections.

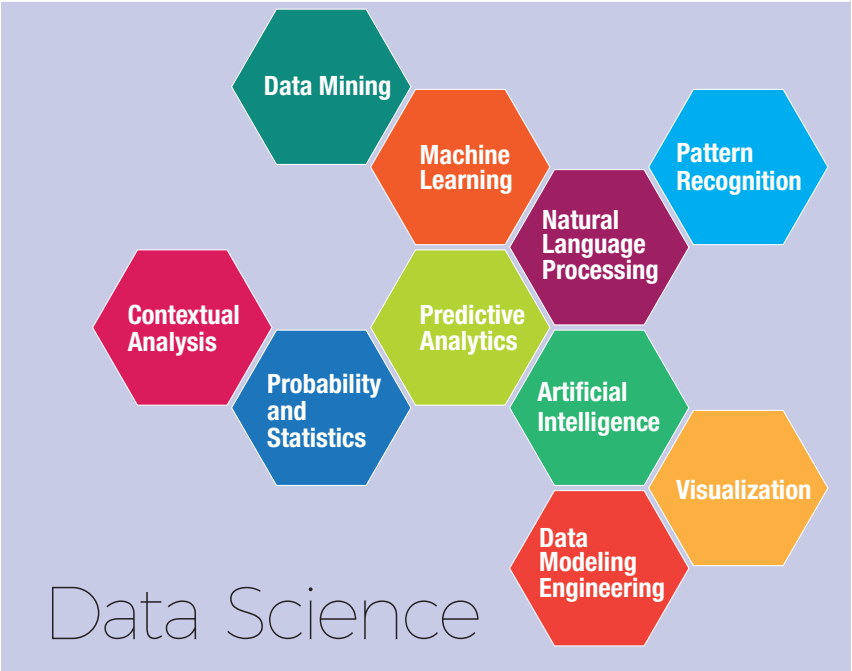
Traditional security solutions are not designed specifically for cloud applications; the protection they afford to on-premises systems does not effectively translate to the cloud. As service providers continue to simplify these features, the threat of data exfiltration (intentional or accidental) increases, making data loss prevention (DLP) an essential feature of any cloud security solution. For example, an advanced on-premises DLP system does not understand link semantics, so it may not

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Aditya K. Sood,** Ph.D.
Is the director of security and cloud threat labs at Elastica, Blue Coat Systems. His research interests are malware automation and analysis, app security, secure software design, and cybercrime. The author of the book *Targeted Cyber Attacks,* he has also authored several articles for IEEE, Elsevier, *CrossTalk*, ISACA®, *Virus Bulletin* and Usenix. Sood has been featured in several media outlets including The Associated Press, Fox News, *The Guardian, Business Insider* and the Canadian Broadcasting Corporation. He has also been an active speaker at industry conferences such as Black Hat, DEFCON, Hack In The Box, RSA, Virus Bulletin and OWASP.

**Michael Rinehart,** Ph.D.
Is a chief scientist at Elastica, Blue Coat Systems, leading the design and development of many of its data science technologies. He has deployed machine learning and data science systems to numerous domains, including Internet security, health care, power electronics, automotives and marketing. Prior to joining Elastica, he led the research and development of a machine learning-based wireless communications jamming technology at BAE Systems.

**Figure 1: Data Science Techniques**




**Source:** A. Sood and M. Rinehart. Reprinted with permission.

recognize that a link sent over email is associated with a file that breaks Payment Card Industry (PCI) compliance.[1] The cause can be as simple as the DLP system not recognizing that it should follow the link or that it simply cannot access the document or interpret traffic from the site.

The question is whether data science can be used as a mechanism to:

- Ensure a user does not accidently expose a file containing compliance concerns
- Prevent and remediate data exposures
- Detect and protect against a malicious insider, attacker or malware posing as an insider

The answer is yes; data science can address all of the listed concerns. This article discusses how cloud security benefits from data science's ability to scale to provide consistent and broad visibility into cloud application usage, interpretable detection of new and dynamic cloud threats, and accurate detection of sensitive content on a cloud service.

## Achieving Visibility

Real-time visibility into cloud applications and related protection requires parsing HTTP traffic to determine:

- The user account accessing the service
- The actions carried out by the user
- The resources (e.g., files) accessed or modified

This information can be extracted using signatures to parse HTTP traffic, resulting in a logged event such as "John Doe shared the document 'passwords.txt' with an external email address." Consider the need to parse HTTPS transactions to gain visibility into network traffic. The HTTPS traffic can be parsed by deploying a transparent proxy that decrypts incoming traffic and simultaneously allows the HTTPS traffic to reach its destination. For example, HAProxy,[2] an open-source proxy and load balancer, can be used in conjunction with Tproxy,[3] a Transmission Control Protocol (TCP) routing proxy to build a full, custom, transparent proxy solution for decrypting HTTPS traffic.[4]

Visibility in traditional network security is typically achieved using static signatures. However, a cloud application changes its network traffic patterns frequently (often at the rate of software sprints, i.e., every couple of weeks), which strains manual signature development. And if securing one application as it evolves is a challenge, securing hundreds or thousands simultaneously, especially as they emerge, is much more difficult. This necessitates approaches to signature generation that adapt as quickly as applications evolve, while simultaneously scaling to the wide breadth of applications available to users. Signatures are typically built by hand—a time-consuming process that is made even more difficult by cloud applications that machine encode critical information such as file names. This is problematic because as cloud applications change their traffic patterns, signatures break and it is costly to rebuild them. Adding to that challenge is the

sheer number of applications available to users requiring individualized signatures. The consequences for security are clear: frequent lack of visibility into how applications are used and, consequently, an inability to identify threats in cloud traffic.

Data science methods (e.g., machine learning, data mining, contextual analysis), however, can scale to meet this challenge by automatically learning signatures that achieve a zero false-positive rate in a fraction of the time required for manual construction. As signatures break, data science techniques can operate within a feedback loop to automatically repair signatures, restoring visibility in a short time. This means that information security teams can confidently expect consistent and deep visibility into user events across a large number of cloud applications.

## Detecting Dynamic Threats

Threats to cloud applications from malicious insiders, attackers and naive users are increasing at a rapid pace. Cloud applications are now being used to host and deliver malware, establish communication channels for data exfiltration, trigger acts of data destruction, expose critical information and hijack accounts. Specific data science algorithms are in a strong position to provide high-quality threat detection when visibility is both rich and meaningful. They are designed to handle large-scale data analysis and thereby extract meaningful information out of the data. Data science can be used as a tool to detect security issues residing in the cloud because intelligence can be gained on multiple fronts as follows:

- **Correlation**—Mapping large sets of data under specific security analytics buckets helps to determine correlation to understand the complete posture of an attack. In addition, when data from multiple locations are correlated, attacks can be dissected at a granular level.
- **Visibility**—Mining of big data means big picture visibility. When large data sets are mined, it becomes easier to obtain visibility into the attacks, which ultimately results in gaining more intelligence.
- **Baseline**—When big data are mined using specific features related to an attack, it helps to generate baselines that can be used to measure the intensity or amplification of attack in a given environment.
- **Context**—Mining big data may provide more adaptive intelligence, including contextual awareness and situational awareness of a specific attack in the environment.

A simple example is as follows:

- Behavior of user (A) is modeled using data science and machine learning to generate baselines.
- User (A) had not shared any file externally through the cloud for the last two to three months, but recently shared a file.
- The behavior of user (A) raises an anomaly alert with deviation ratio from the generated baseline (probability) computed earlier.
- Additional security components are executed to analyze the generated anomaly for potential threats. For example, deep content inspection (DCI) dissects the anomaly to detect if any sensitive compliance-related data, such as personally identifiable information (PII), PCI or protected health information (PHI), is leaked through the document.

- A risk score is calculated and the threat is detected accordingly.

Data science algorithms can also meaningfully integrate multiple information sources to provide a more complete picture of a user's estimated risk to an organization. Such algorithms automatically scale horizontally as the number of input signals (users, applications, actions, locations and devices) increases. Meaningful visibility that logs user actions allows for meaningful threat detection. For instance, an alert such as "John Doe viewed an abnormally high number of contacts in Salesforce" may be very important to the information security team if they discover that John Doe is not in sales.

**"The potential for "noise" in the cloud is far higher than for on-premises systems, and such noise increases the rate of costly false-positive alerts."**

Data science algorithms reduce the burden on the information security team to develop policies that can detect aberrant behavior while achieving low false-positive rates. This is because they are able to scale to develop user-level behavioral models across applications, actions and even information categories (e.g., files, folders, documents, blogs) with high fidelity.

## Building Cloud Generation Data Loss Prevention Solutions

In traditional security, data exfiltration is addressed by data loss prevention (DLP) systems that scan in-flight emails and files stored on servers.[5] Such systems can effectively rely on regular expressions, key words and file extensions to identify sensitive information. There are a number of traditional DLP solutions provided by companies such as Symantec,[6] Fortinet,[7] McAfee,[8] Checkpoint,[9] Websense,[10] EMC[11] and TrendMicro[12] that use standard techniques to handle data leakage. The data stored in the cloud, however, are different than data stored in on-premises servers because employees use the cloud for a much wider variety of activities. For example, a file-sharing service can contain a vast amount of short information snippets (passwords or text from the Internet); archives such as emails, receipts and network logs; media files; drafts of sensitive documents that have not been tagged; and official documents such as employee forms and customer invoices.

The potential for "noise" in the cloud is far higher than for on-premises systems, and such noise increases the rate of costly false-positive alerts. Data science techniques can address this challenge by leveraging increased information from documents when evaluating them. For example, finding a nine-digit number in a health form is more likely to constitute PII than, say, a nine-digit number contained in a network log or in the raw text of an email. By using context, data science algorithms maintain high sensitivity with lower false-positive rates.

Data science further broadens the range of sensitive documents identifiable by a DLP system, and it does so while reducing administration efforts. For example, data science can detect untagged design and financial documents using document structure and natural language processing. It uses data science techniques to offer broader and more effective detection of source code without relying on highly specific key-word combinations that reduce overall sensitivity.

Finally, there is the challenge posed to DLP systems by the vast size and range of content stored in the cloud. Prior to the cloud, many user files resided locally, while more important company files were shared or archived. However, the convenience of the cloud results in employees using it to store many file types that were once stored locally, including emails,

receipts, password and certificate files, downloaded files, and event logs. The sheer volume of "noise" results in a far greater source of potential false positives. To be of value to an information security team, cloud DLP must maintain and improve its ability to detect sensitive content without increasing the false-positive rate.[13]

## Applying Automatic Prevention and Remediation Policies

Data science's benefits of improved visibility and improved accuracy provide new opportunities for information security teams to define automatic policies to protect the contents of their cloud applications. Real-time visibility can be used to block certain cloud applications' actions. When combined with advanced threat detection, at-risk user accounts can be automatically restricted until cleared by the information security team. Finally, rapid remediation can take place as well—if a user were to share a sensitive file, the system can automatically unshare it. Aside from policies, granular event logging provides the information security team with increased potential for root-cause analysis, which can help uncover new or broader threats to the network.

## Conclusion

A combination of port and application blocking has been successful in mitigating a variety of network attacks in cases where enterprise-sanctioned applications are deployed on-premises. But as enterprises move to the cloud, these mechanisms become less effective. There is now a need to proactively protect enterprise-sanctioned cloud applications at a level of granularity that detects and blocks malicious actions while facilitating productivity. Data science is a tool that helps scale current expert-driven security practices and technologies to the size and speed of cloud applications. Specifically, it leads to improved visibility into user actions on cloud applications, interpretable detection of potential threats, and both deeper and broader detection of sensitive content. These benefits reduce the burden on information security teams by reducing false-positive alerts without sacrificing sensitivity to threats, and they further facilitate confident usage of automatic prevention and remediation policies.

## Endnotes


1 SANS Institute, Data Loss Prevention, USA, 2008, *www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883*
2 HAProxy, *www.haproxy.org*
3 GitHub, *github.com/benoitc/tproxy*
4 Turnbull, M.; "Configure HAProxy With TPROXY Kernel For Full Transparent Proxy," loadbalancer.org, 11 February 2009, *www.loadbalancer.org/blog/configure-haproxy-with-tproxy-kernel-for-full-transparent-proxy*
5 Elastica, *The 7 Deadly Sins of Traditional Cloud Data Loss Prevention (DLP) in the New World of Shadow IT*, 2014, *https://www.elastica.net/ebook-7sins-dlp/*
6 Symantec, "Data Loss Prevention," 2015, *www.symantec.com/products/information-protection/data-loss-prevention*
7 Fortinet, "Data Leak Prevention (DLP)," *Inside FortiOS*, 2013, *http://docs.fortinet.com/uploaded/files/1118/inside-fortios-dlp-50.pdf*
8 McAfee, "McAfee Total Protection for Data Loss Prevention," *www.mcafee.com/us/products/total-protection-for-data-loss-prevention.aspx*
9 Check Point, "Data Loss Prevention Software Blade," *www.checkpoint.com/products/dlp-software-blade*
10 Websense, "Websense Data Security Suite," 2013, *www.websense.com/assets/datasheets/datasheet-data-security-suite-en.pdf*
11 RSA, "Data Loss Prevention Suite," *www.emc2.bz/support/rsa/eops/dlp.htm*
12 Trend Micro, "Integrated Data Loss Prevention (DLP)," *www.trendmicro.com/us/enterprise/data-protection/data-loss-prevention*
13 Elastica, "Cloud Data Loss Prevention (Cloud DLP)," *www.elastica.net/data-loss-prevention*




# Network Access Control—Has It Evolved Enough for Enterprises?

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Trevor J. Dildy,** CCNA
Is a member of the classroom technology team at East Carolina University (USA). The team is responsible for researching the latest state-of-the-art hardware and software for ECU classrooms. He is a former member of the IT security team at Vidant Health, assisting with access administration requirements for the health system.

Information security is a field that continues to grow and mature. As technology advances, there will always be growth in new security techniques or solutions to help protect data from various attacks. Network access control (NAC) is the technique for network management and security that enforces policy, compliance and management of access control to a network. It also monitors and controls activity once devices and/or people are on the network.

Over the years, NAC has grown and many companies, such as Cisco, Trustwave and Bradford Networks, have developed solutions to help with its evolution. However, not all organizations believe that NAC has evolved to fit their needs. While NAC is an important part of information security and can help with data breaches, is it truly ready to be used in all enterprises or does it need to develop into a more usable technical solution before it is utilized everywhere?

## Reasons to Implement NAC

Enterprises have a lot of reasons to consider implementing NAC. When it comes to access controls, they need to have a wide range of options. But perhaps the pertinent question is whether or not enterprises are even ready to be utilizing NACs. NACs can be expensive to implement, but expense should not be an excuse to ignore the fact that threats are frequently trying to compromise enterprise systems.

One of the top reasons for implementing NAC, is bring your own device (BYOD) threats.[1] With more and more employees taking their own devices to work and using them for work purposes, NAC is becoming more in demand. There are many variations of mobile devices; some of the top operating systems are Apple iOS, Android and Windows. There are hundreds of combinations that deal with device type (e.g., smartphone, laptop and tablet) and model. Each of these smart devices now comes with a huge selection of applications (apps) that can be downloaded onto them.[2] There are many possible threats, especially since these personal devices do not typically have enterprise-level antivirus/antimalware or mobile device management (MDM) solutions installed.

Most NAC technical solutions are able to support the major operating systems on the market today. These solutions can automatically detect devices as they connect to the network and then make sure that they are not compromising the security that is in place. NAC is very useful when it comes to protecting the integrity of the network, but it can also help with allowing or denying access to the network. Active directory is the best implementation option for allowing and denying access to the network.

> **“NAC is very useful when it comes to protecting the integrity of the network, but it can also help with allowing or denying access to the network.”**

Delivering role-based network access is another reason for moving to a NAC scenario.[3] As IT professionals know, having to deal with a large amount of network share permissions in a very large organization can be a difficult task. A NAC product solution makes it a little more bearable to manage all of the permissions that are needed for network storage folders as well as other active directory groups.

A third reason for implementing NAC in an organization, is reducing the risk from advanced persistent threats (APTs).[4] NAC does not provide any sort of solutions that will detect and stop APTs, but it can stop the attacking source from gaining access to the network.[5] This means that if a user account is causing an attack, the NAC can stop that account from causing any further harm if the NAC system detects any foul play.

When implemented correctly, NAC can help an organization feel in control of the network and the devices connected to it, especially with the huge numbers and types of devices that are being used.

## NAC Products

Cisco TrustSec, from worldwide IT industry leader Cisco, simplifies the provisioning of network access. Cisco TrustSec is embedded in the Cisco infrastructure that many organizations already use.[6] This solution comes with a firewall; the NAC portion comes as a separate component. This allows for easier security policy management and helps the organization manage network access.

The Cisco NAC solution helps by recognizing the users who are on the network, as well as their devices and roles. Another feature of the Cisco NAC solution is that it provides guest access and makes sure that the access provided is safe and secure. This is a valuable feature for anyone who is looking to implement a NAC system.

Another feature is that auditing and reporting are enabled. This allows for the tracking of who is on the network as well as making sure they do not try to gain unauthorized access to restricted parts of the network to which they should not have access. The features that Cisco's NAC system offers are very beneficial for most organizations that are willing to implement NAC systems.

There are other companies that have NAC products that can help organizations keep access limited to those who truly need it or base the access on the job that they need to perform each day. Trustwave Network Access Control, offered by global managed security services leader Trustwave, can be deployed seamlessly without an agent. Like most NAC products, it can be integrated into the active directory in order for it to be easier to determine who has what access.

According to Trustwave, its NAC solution has automated detection and restriction of noncompliant devices, as well as complete protection for all endpoints—managed and unmanaged. This is a very bold statement when it comes to NAC products.[7] Also, Trustwave claims that analysis of every packet from every device can be done. While it is possible to analyze many packets, it is hard to claim that there is a way to analyze every packet that comes through the NAC.

There are a few options in implementing the Trustwave product as outlined in **figure 1**. Like the Cisco NAC solution, Trustwave offers integrated support for BYOD. BYOD integration from Trustwave will help with device identification, authentication, categorization and threat mitigation. Trustwave helps organizations make the BYOD solution decision by providing a side-by-side comparison of its different options. The solutions they offer are an enterprise NAC, a managed NAC and a plug-and-play NAC. Each of the solutions has its own benefits. The plug-and-play option is an add-on software module that goes with the Trustwave managed unified threat management

**Figure 1—Options in Implementing Trustwave**

| TS-25 | TS-150 | X2500 |
|---|---|---|
| • Protects up to 100 endpoints<br>• Up to 64 virtual local area networks (VLANs)<br>• Can be installed on a desktop computer<br>• Option to include the rack mount kit | • Protects up to 1,000 endpoints<br>• Up to 128 VLANs<br>• Needs to be installed on one rack unit (1RU) rack mount | • Protects up to 2,500 endpoints<br>• Up to 128 VLANs<br>• Needs to be installed on a 1RU rack unit |

**Source:** Trevor J. Dildy. Reprinted with permission.

## Enjoying this article?

- **Learn more about, discuss and collaborate on access control and network security in the Knowledge Center.**
  *www.isaca.org/knowledgecenter*

(UTM) service. The managed NAC is similar to the enterprise NAC, but it is at a reduced cost and will not incur any capital expense. The enterprise NAC provides all the features and costs more than the other two options.

Trustwave offers numerous benefits, but it also has some very big claims that should be explored further. Trustwave's NAC products seem to be very good at what they do, and they will protect an organization's network without having to worry about an agent.

ForeScout Technologies is a global provider of continuous monitoring and mitigation solutions. ForeScout's NAC solution is CounterACT. This solution allows the organization to have real-time visibility of the people, devices, operating systems and apps that are connected to the network. The CounterACT solution will not disrupt users' daily operations; it will actually make sure that operations are not disrupted while giving the user automated controls to help preserve the experience of the user.[8]

CounterACT is different from some of the solutions on the market now as it is basically a turnkey solution. Everything within the CounterACT solution is contained in a single physical or virtual machine. This means that the setup is fast and easy. CounterACT also works with a majority of the routers, switches and firewalls that are on the market today. Like Trustwave's NAC, CounterACT is agentless, which means it can identify, classify, authenticate and control network access for devices whether they are managed or unmanaged.

CounterACT is also nondisruptive; this means it can be deployed in a phased approach. This will allow users to continue working without having to worry about losing access to critical files. A useful feature of CounterACT is the ability to decide what happens with devices that match certain parameters. When dealing with those parameters, there are three levels of control options: alert and remediate, limit access, and move and disable.[9] When it comes to alert and remediate, the system alerts when it detects an incident and triggers other endpoint management systems to remediate the issue. Limit access deploys a virtual firewall around the selected device and takes action to either restrict access completely or put it on a preconfigured guest network. The strictest parameter, move and disable, moves the device to a quarantined VLAN and blocks access to the network from the device.[10] With ForeScout's solution being one of the quickest and easiest to set up, deploy and integrate, it can be considered one of the top solutions that could potentially be implemented on a network.

When it comes to selecting NAC products, enterprises should choose the solution that best fits their network's needs. In addition to considering all of the costs, it is best not to select a solution that is designed for a smaller network.

## Advantages and Disadvantages of Implementing NAC

There are some arguments for, as well as against, the implementation of NAC. There are some compelling arguments that show that NAC should be installed on many of the organizations' networks so that those networks can have the proper protection against looming threats. One of the benefits is that it will stop malicious actors from being able to plug into the organization's network infrastructure. With employees and users bringing their own devices into the workplace, it is easy for them to also bring the necessary cable(s) in order to connect to one of the empty Ethernet ports and try to gain access to the network. NAC will help to prevent this from happening because the device that they are trying to connect to the network is not listed on the approved list or has not been registered as a trusted device within the NAC.

Another plus for NACs are that there are audit logs that can determine if empty ports are turned on or off. This can help the organization determine if there are some ports that were left on that should be taken offline so no one mistakenly connects to them. NACs also allow for the detection of devices that are plugged into the network's infrastructure that should not be.

NAC integrates well with other solutions. NACs are not meant to be stand-alone solutions; they are supposed to work in conjunction with firewalls and other security solutions to help improve the overall security measures of the organization. NACs are

needed to help an organization be more secure in relation to who has access and who should not have access. This also helps to minimize the number of breaches to the network.

It can be difficult to find the appropriate NAC product that best fits into the enterprise's network infrastructure. NACs have come a long way from where they used to be, but this does not mean that all enterprises are ready to implement them into their network. Like most software solutions, there are some benefits to NACs and some drawbacks. It is important to consider the downsides when deciding on a NAC solution.

It has been said that endpoint security checks work only when you need them least.[11] What this means is that NACs tend to work well when they are used to monitor laptops and desktops, but not so well when they are needed to monitor other devices/users coming into the enterprise. Another drawback is that, in general, NACs are always preparing to fight the last war, not preparing for the next one. NACs focus on the threats from the previous week. While this is beneficial, it is not what needs to be happening when it comes to advanced security threats. NACs need to be able to focus on the threats of tomorrow in addition to the threats of last week.

The return on investment (ROI) on NACs is a big unknown. While it might be crucial to have a NAC connected to the network, it might not yield the expected ROI. Putting a NAC in place is not cheap; it is very expensive and might prove to not be worth it for some organizations.

Another failure:  Too much information can sometimes overload a NAC.[12] With a NAC, an organization can set its own policies for each user. This could result in a lot of policies, which would eventually yield a great deal of information that is not needed at the time or cause the NAC to generate false alerts.

Another NAC failure is that the network can control only what is seen.[13] With some of the NAC solutions allowing users access to officially permitted servers, this causes a huge hole in the NAC configuration. When anyone can have access to permitted servers, the server may become what is called a "jumping point" that will allow users to cruise the network and access other network objects or shares.[14] It is easy to get into the network when the MAC address is faked to the host. When it is faked, it will let the user or attacker into the network. Significant threats can come from the inside or outside because there is little to no physical security. Without proper physical security, it is easy for anyone to gain access to the NAC and harm its functionality. If there is no failover scenario, it is very likely that the organization will cause a denial-of-service (DoS) situation for itself—the same type of threat that the organization is trying to avoid.

**"NACs need to be able to focus on the threats of tomorrow in addition to the threats of last week."**

NACs are also hard to manage with large numbers of switch ports because it is difficult to make sure that the switch ports are configured correctly all of the time. This can be harmful to the network. It is very important to make sure that, even where there are many ports, they are all configured correctly.

## Conclusion

All of the necessary research needs to be completed to determine what exactly the network requires to be as secure as possible. After the research on the proper product has been conducted, the pros and cons can be weighed and the decision made whether the cost of the NAC is acceptable to the organization. Cisco, Trustwave and ForeScout have NAC solutions that can be beneficial to any network; however, full realization of the benefits depends on fitting the solution to the network infrastructure currently in place. NACs will help to limit the access devices have and users are given. Access is determined based on users' job roles, which helps ensure that their access to network storage aligns with what they need to complete their job—not what they believe they need. NAC is not required, but it can save the organization damage to reputation, legal fees and additional work required after experiencing a breach.

## Endnotes


1 Shapland, R.; "Three Reasons to Deploy Network Access Control Products," *TechTarget*, 7 April 2015, *http://searchsecurity.techtarget.com/feature/Three-reasons-to-deploy-network-access-control-products*
2 *Ibid.*
3 *Ibid*.
4 *Ibid*.
5 Boscolo, C.; "How to Implement Network Access Control," *ComputerWeekly.com*, November 2008, *www.computerweekly.com/opinion/How-to-implement-network-access-control.*
6 Network Admission Control, Cisco, *www.cisco.com/c/en/us/solutions/enterprise-networks/network-admission-control/index.html*
7 Trustwave Network Access Control, *www.trustwave.com/Products/Network-Security-and-Access-Control/Network-Access-Control/*
8 Network Access Control (NAC), ForeScout, *www.forescout.com/solutions/network-access-control/*
9 Snyder, J.; *NAC Deployment: A Five Step Methodology, Opus One*, February 2007, *www.opus1.com/nac/vendorwhitepapers/opusone_nacdeployment.pdf*
10 *Ibid*.
11 Snyder, J.; "The Pros and Cons of NAC," *NetworkWorld*, 12 June 2006, *www.networkworld.com/article/2304152/lan-wan/the-pros-and-cons-of-nac.html*
12 *Ibid*.
13 *Ibid*.
14 *Ibid*.

# Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous



Mobile computing devices (i.e., laptops, tablets and smart phones) can cause serious harm to organizations and to device owners, their friends and families, because mobile devices are far less secure than desktops and laptops. The *Verizon 2015 Data Breach Investigations Report*[1] states that there are tens of millions of mobile devices. And, according to Statista,[2] there will be 4.77 billion mobile phone users in 2017 and 1.15 billion tablets in use in 2016.[3] As the number of mobile computing devices increases, so do mobile security concerns. There are already many existing and new threats related to mobile devices.

This article discusses the actors, threats, vulnerabilities and risk associated with mobile computing devices and highlights the pervasiveness of security and privacy problems and issues.

## Actors

The actors (aka threat vectors) include the device itself, the applications (apps) on the device, compromised web sites, wireless data connections, other users and organizations, the organization to which the device user belongs, and the service providers.

## Mobile Computing Device Threats

Newly purchased mobile devices can be configured insecurely. Devices can contain the original vulnerable operating system (OS) that has not been updated to eliminate known vulnerabilities. If a device does not require some type of access controls such as a personal identification number (PIN) or fingerprint, it is ripe for unauthorized use by anyone who has access to it. There are many types of malware that can provide people with malicious intent the ability to obtain sensitive data stored on a device. Protecting data can be more of a problem if one makes the mistake of loading sensitive organizational information on it. Users need to be aware that they are responsible for protecting the device, preventing physical tampering, setting security-specific features, and avoiding supply chains that provide compromised or unsecure mobile devices.

If a mobile device has an attachment to read credit cards, it, too, can be compromised by a technique known as skimming.[4] A smartphone can perform surveillance via its audio, camera and Global Positioning System (GPS) capabilities, as well as recording call logs, contact information and Short Message Service (SMS) messages. Mobile computer devices can cause financial problems because, if compromised, they can send premium SMS messages, steal transaction authentication numbers, allow extortion via ransomware and make expensive calls without the device owner's knowledge. A device can even be hijacked and turned into a distributed denial-of-service (DDoS) bot, making it harder for organizations to detect and prevent such DDoS attempts.

App-based threats include malware, spyware, vulnerable apps, compromised apps and data/information leakage due to poor programming practices. The types of app attacks include:

- Disabling or circumventing security settings
- Unlocking or modifying device features
- Apps that were obtained (free or purchased), but contained malicious code

Examples of malware capabilities include:

- Listening to actual phone calls as they happen
- Secretly reading SMS texts, capturing call logs and emails
- Listening to the phone surroundings (device is used as a remote bugging device)
- Viewing the phone's GPS location
- Forwarding all email correspondence to another inbox
- Remotely controlling all phone functions via SMS

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Larry G. Wlosinski,** CISA, CISM, CRISC, CAP, CBCP, CCSP, CDP, CISSP, ITIL v3
Is a senior associate at the Veris Group LLC and has more than 16 years of experience in IT security. Wlosinski has been a speaker on a variety of IT security topics at US government and professional conferences and meetings, and has written numerous articles for professional magazines and newspapers.

## Enjoying this article?

- Read ***Security Mobile Devices Using COBIT® 5 for Information Security.*** *www.isaca.org/securing-mobile-devices*
- **Learn more about, discuss and collaborate on mobile computing in the Knowledge Center.** *www.isaca.org/topic-mobile-computing*

- Accepting or rejecting communication based on predetermined lists
- Evading detection during operation

A compromised web site can be a danger to everyone's information. It can be the source of phishing scams, drive-by downloads of malware and browser exploits. Wi-Fi via free hotspots can provide criminals the means to obtain banking access and financial account information. These web sites can be used to obtain personal data about device owners, their families and friends, and the places they work. Vulnerabilities to avoid include keeping a Wi-Fi connection enabled at all times, not using or enabling a device firewall, browsing unencrypted web sites, failing to update security software, and not securing home Wi-Fi.

Data communications via a personal or company network can also be a nonsecure means of communications. The communication problems include video, audio and data that can be collected over the air by an insecure network. There are many types of network exploits including Wi-Fi sniffing, manipulation of data in transit, data exposure through radio frequency (RF) emission, connection to an untrusted service, signal jamming and flooding, and monitoring a GPS/geolocation. All of these threats need to be avoided.

User-based threats include: social engineering, inadvertently (or intentionally) releasing classified information, theft and/or misuse of device and app services, and malicious insiders who steal devices for their own purposes or for someone else.

Social engineering can be accomplished by:

- **Phishing**—Masquerading as a trustworthy entity
- **Vishing**—Tricking a victim into calling a phone number and revealing sensitive information
- **Smishing**—Tricking someone via messaging into downloading malware onto their mobile device
- **Exploiting Social Media Accounts**—Using shortened malicious web site names (to describe one example)

Your own organization's network infrastructure can be a threat. Used maliciously, a wireless network can pose threats such as:

- Providing a means for unauthorized access
- Permitting or promoting the installation of malware
- Permitting the loss of data integrity of the system and associated databases
- Spreading compromised apps
- Acting as the source of insecure coding
- Permitting eavesdropping, data interception, voice/data collection, drive-by downloads, location tracking (via GPS) and behavior tracking

An Internet service provider (ISP) can also be a threat to individuals and organizations. The ISP gathers and stores device location; device ownership information; application usage behavior; email routing/forwarding information; information about purchased music, movies, TV shows, apps and books; and sensitive internal reports. All of this information can be stored in the cloud for years.

Other information that can be kept in the cloud for a long time includes: photos and videos; personal contact information, calendar events, reminders and notes; device settings; application data; Adobe PDFs; books added to an order list; call history; home screen and application organization; text and email messages; ringtones; home system security settings (HomeKit[5] data ); personal health information (HealthKit[6] data ); and voicemail.

## Vulnerabilities

Mobile computing device vulnerabilities exist in the device itself, the wireless connection, a user's personal practices, the organization's infrastructure and wireless peripherals (e.g., printers, keyboard,

mouse), which contain software, an OS and a data storage device.

If not secured by encryption, wireless networks often pass sensitive information in the clear that can do harm to individuals and/or organizations. Unintentionally released sensitive data can not only affect the organization's reputation and the lives of those affected, but can also be the cause of legal action. Wireless communications can carry and install malware on any computing device configured to receive it. This malware can cause data corruption, data leakage, and the unavailability of services and functionality. Personal privacy can also be affected if the audio (e.g., Bluetooth) and video/picture communication (e.g., device camera) are intercepted and used with malicious intent. The wireless protection provided by an organization will work only if a user is in the organization's network perimeter where the security controls are in place.

Unencrypted organization, customer and employee information stored on the computing device can inadvertently be made available to others if someone intercepts it while in transit or if the device is stolen (and no access controls are in place). It is not difficult to intercept wireless communications traffic because there are free tools available on the Internet to help hackers do this.

In this age of wireless technology, many roles (e.g., doctors, medical support staff, retail and wholesale inventory personnel, registration support staff) depend on mobile computing devices to efficiently capture and transmit data. The users of these devices rely on them for their productivity and livelihood. In many cases, the information is sensitive to the organization and, if it is employee- or customer-related, it can be personal and privacy-related (i.e., personally identifiable information [PII]).

If one's organization does not have a wireless encryption program (i.e., virtual private network [VPN]) in place, then mobile devices may interact with personal devices' email and obtain sensitive correspondence. The lack of encrypted communication can allow malware to access the network and propagate Trojans and viruses throughout the organization. More serious is the fact that it can allow intrusion into the enterprise, which can then compromise the entire organization. Remember that a VPN connection requires authentication—a critical protective control—to permit network access.

**"If not secured by encryption, wireless networks often pass sensitive information in the clear that can do harm to individuals and/or organizations."**

## Application Vulnerabilities

Other vulnerable components of the mobile computing device environment are the apps loaded on it. Each application can contain a vulnerability that is susceptible to exploitation. The apps on the mobile device can have a variety of vulnerabilities including:

- Incorrect permission settings that allow access to controlled functionality such as the camera or GPS
- Exposed internal communications protocols that pass messages internally within the device to itself or to other applications
- Potentially dangerous functionality that accesses the resources or the user's personal information via internal program data calls or hard-coded instructions
- Application collusion, where two or more applications pass information to each other to increase the capabilities of one or both applications
- Obfuscation, where functionality or processing capabilities are hidden or obscured from the user

- Excessive power consumption of applications running continuously in the background, which drain the battery, thereby reducing system availability
- Traditional software vulnerabilities such as insufficient editing of data entered, Structured Query Language (SQL) query exploitation and poor programming practices
- Privacy weaknesses in configuration settings that allow access to the application's sensitive information (e.g., contacts, calendar information, user tasks, personal reminders, photographs, Bluetooth access)

## Risk

The most common risk factors that apply to using mobile devices are: computer viruses, worms or other personal computing device-specific malware; theft of sensitive data; exposure of critical information through wireless sniffers; wireless intruders capturing emails, email addresses and attached data (if the security safeguards are insufficient); loss, theft or damage of the device; use of the device as a proxy to establish a virtual connection from an attacker to an internal network; data loss/leakage due to the small size and portability; fraud enabled by remote access or copying mass amounts of sensitive data; spam causing disruption and driving up service costs if targeted toward mobile devices; and malformed SMS messages causing devices to crash.

## Conclusion

Each day, mobile device attack vectors are continuously undergoing dynamic changes, and it is difficult to represent a complete set of the threats and vulnerabilities. With the development of mobile computing devices that can be carried in a pocket or a duffle bag comes the responsibility to protect those devices and the data within them. Being aware is only the first step in the fight to protect the data.

## References


Lookout, "What Is a Mobile Device Threat?," *https://www.lookout.com/resources/know-your-mobile/what-is-a-mobile-threat*

Mobile App Security Guide, infographic, *http://autosend.io/mobile-app-security-guide/*

Wysopal, C.; "Mobile App Top 10 List," Veracode, 13 December 2010, *www.veracode.com/blog/2010/12/mobile-app-top-10-list*

European Union Agency for Network and Information Security, "Top 10 Smartphone Risks," *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks?_ga=1.234877470.1254580284.1439215552*

Quirolgico, S.; J. Voas; T. Karygiannis; C. Michael; K. Scarfone; *Vetting the Security of Mobile Applications*, Special Publication 800-163, National Institute of Standards and Technology (NIST) USA, 2015, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf*

Althuser, J.; "7 Ways Hackers Can Use Wi-Fi Against You," *CSO*, 9 November 2015, *www.csoonline.com/article/3003220/mobile-security/7-ways-hackers-can-use-wi-fi-against-you.html*

Apperian, "Mobile App Security," *https://www.apperian.com/mobile-application-management/mobile-app-security/*

ISACA, *Securing Mobile Devices*, USA, 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx*

Milligan, P. M.; D. Hutcheson; "Business Risks and Security Assessment for Mobile Devices," *ISACA® Journal*, vol. 1, 2008

Absolute, US Mobile Device Security Survey Report 2015, *https://www.absolute.com/en/resources/whitepapers/mobile-device-security-survey-report-us*

## Endnotes

1 Verizon, *2015 Data Breach Investigations Report*, 15 April 2015, *www.verizonenterprise.com/DBIR/2015/*
2 Statista, "Number of Mobile Phone Users Worldwide From 2013 to 2019 (in Billions)," 2016, *www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/*
3 Statista, "Number of Tablet Users Worldwide From 2013 to 2019 (in Billions)," 2016, *www.statista.com/statistics/377977/tablet-users-worldwide-forecast/*
4 Skimming is the capturing of credit card information using a card reader that records and stores the user's card information.
5 Apple, HomeKit, *www.apple.com/ios/homekit/?cid=wwa-us-kwm-features*
6 HealthKit, *https://www.healthkit.com/*

# Managing Cloud Risk

## Top Considerations for Business Leaders

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

**Phil Zongo**
Is a cybersecurity consultant based in Sydney, Australia. He has more than 10 years of technology risk consulting and governance experience working with leading management consulting firms and large financial institutions. He recently led a successful risk assessment initiative for a complex, multimillion-dollar cloud transformation program.

Cloud adoption continues to grow at a rapid pace, transforming businesses across the globe. In fact, cloud is now business as usual for most organisations, with some utilising it to run business-critical processes. In July 2015, the ISACA® *Innovation Insights* report[1] cited cloud computing as one of the leading business trends driving business strategy. It ranked third out of 10 top emerging technologies most likely to deliver significant business value in excess of cost. Big data analytics and mobile technologies ranked first and second, respectively. A separate publication by International Data Corporation (IDC) forecasts worldwide use of public cloud growing at 19.4 percent annually over the next five years, nearly doubling from approximately US $70 billion in 2015 to more than US $141 billion in 2019. This is almost six times the growth of enterprise IT spending as a whole.[2]

Whilst cloud promises significant benefits, including enhanced financial flexibility, improved agility and access to leading technologies, some organisations are still holding back, mostly wary of losing control over high-value information. These risk concerns are valid and, if not properly considered and managed, may result in detrimental business impacts, including degraded customer experience, sensitive data breaches or brand damage.

This article provides some practical recommendations to address three key areas of risk associated with cloud adoption:

1. Cloud initiatives not aligned with business strategies
2. Loss of control over high-value information
3. Overreliance on cloud service providers

This is not a definitive or complete set of risk areas that businesses might face when adopting cloud computing. Several frameworks, most notably from the Cloud Security Alliance (CSA), ISACA®, and the US National Institute of Standards and Technology (NIST), provide more comprehensive guidance on managing cloud risk.

### Aligning Cloud Projects With Business Strategy

Enterprises deliver shareholder value by taking on risk, but fail when the risk is not clearly understood and effectively managed. Often, cloud projects are IT-driven and technology-centric. To deliver business value and minimise risk exposure, such initiatives should be fully aligned to business strategies. Active engagement and oversight by the board or relevant risk governance committees are essential prerequisites for cloud program success.

In its June 2012 publication, *Enterprise Risk Management for Cloud Computing*,[3] the Committee of Sponsoring Organizations of the Treadway Commission (COSO) emphasised that the responsibility for cloud risk management starts right at the top. The paper stated, 'Cloud computing should be considered in the organization's overall governance activities and regarded as a topic warranting discussion and inquiry by an organization's board'. The board should determine what cloud services are appropriate to the business, based on enterprise goals, risk appetite and tolerance. But this is not always the case.

The Australian Prudential and Regulatory Authority (APRA), in a cloud information paper published in July 2015,[4] raised a concern that cloud reporting by regulated entities to boards of directors (BoDs) mostly focused on the benefits, while failing to provide adequate visibility of associated risk. Effective cloud risk management requires the board to challenge the adequacy of risk measures against appetite and business strategy. To enable this, pertinent information should be provided, including:

- Cloud value proposition, traceable links to business strategy and how benefits will be measured
- Top business risk and treatment strategies, i.e., data security, privacy laws, data location, business resilience, regulatory compliance
- Proposed cloud deployment model: public, private or hybrid and associated risk implications
- Planned cloud service delivery model: Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), and associated risk implications
- Service provider selection criteria, including financial viability, operational stability and cybersecurity capabilities
- Plausible business disruption scenarios and recovery plans

- Service level agreements (SLAs), incident response and operational governance
- Third-party assurance, penetration testing, vulnerability assessments and right-to-audit clauses

Cloud initiatives should start with identifying business problems and strategic objectives and then build solutions to address business-specific needs. Clear, ongoing communication of cloud value and the risk management approach is critical to gaining business buy-in into cloud programs and achieving their ultimate success.

## Protecting High-value Information

Managing cyberrisk without restricting business innovation and agility is a critical business imperative. Although cloud providers continue to invest heavily in security capabilities, concern about data security and regulatory compliance remains one of the key barriers to cloud adoption. In 2015, The Economist Intelligence Unit, in collaboration with IBM, conducted a global cloud maturity study. The results of this multiphased research, which reflected upon the perspectives of 784 stakeholders (including board members, chief executive officers [CEOs], chief financial officers [CFOs], chief information officers [CIOs] and other C-level executives) globally, revealed data security as the top likely negative influence to cloud adoption over the next three years, proving that some business executives are not yet convinced about cloud security. These concerns are further heightened by new risk presented by elements of the public cloud, in particular:[5]

- **Multitenancy**—Computing capacity, storage and network are shared across multiple cloud customers. Whilst this model allows cloud providers to achieve economies of scale and lower service costs, there is increased risk that a single vulnerability or misconfiguration can lead to a compromise across multiple customers.
- **Shared responsibilities**—Migrating business applications to the cloud creates a model of shared responsibilities between cloud customers and service providers. Customers relinquish some key responsibilities to the service provider, e.g., physical access and infrastructure management.

The European Union Agency for Network and Information Security (ENISA) asserts that massive concentrations of resources and data in the cloud present a more attractive target for cybercriminals.[6] Furthermore, cloud security breaches garner wider media coverage, which amplifies the impact of such incidents. Extensive media coverage of the 2014 Apple Cloud breach, which exposed pictures of celebrities, underscores this point.

There are three critical security controls to protect high-value information in the cloud: information classification, encryption and privileged access management.

**Identify High-value Information Assets**
Data classification is a vital step toward building an effective cloud security control environment. Information owners should be engaged to assess and classify information assets based on business risk. This eliminates unnecessary security expenditure, as more resources are invested to protect the 'crown jewels'.

Data criticality differs from one organisation to the next, depending on the industry sector or corporate objectives. Insurance companies, for example, may be concerned with the privacy of their customers' health information, whilst high-tech firms may be concerned about the security of their product development plans.

Information that would be of high value to cybercriminals should also be considered. In September 2014, a Reuters article stated that medical information is now worth 10 times more than credit card numbers on the black market and is increasingly being targeted by cybercriminals.[7] Other high-value information targeted by cybercriminals includes business plans, pricing models, partnership agreements, emails for business executives and personal financial records.

As illustrated by **figure 1**, classifying information enables business leaders to make informed decisions regarding how much risk they want to take in pursuit of innovation. For example, an organisation may have no appetite to host highly confidential information in public cloud systems, yet have the appetite to utilise public cloud systems to host public information.

### Isolate High-value Information

Once data has been classified, regulated enterprises may consider using a private cloud to isolate high-value applications. Private clouds, where a business owns and manages its own virtual environment, offer an opportunity to realise the benefits of the cloud whilst eliminating multitenancy and shared responsibility concerns. Previously, some organisations avoided private clouds due to the high set-up costs. The Verizon *2016 State of the Market—Enterprise Cloud Report* revealed that the cost of a private cloud is decreasing, providing organisations with safer, cost-effective environments to host high-value systems.[8]

### Encrypt Sensitive Data

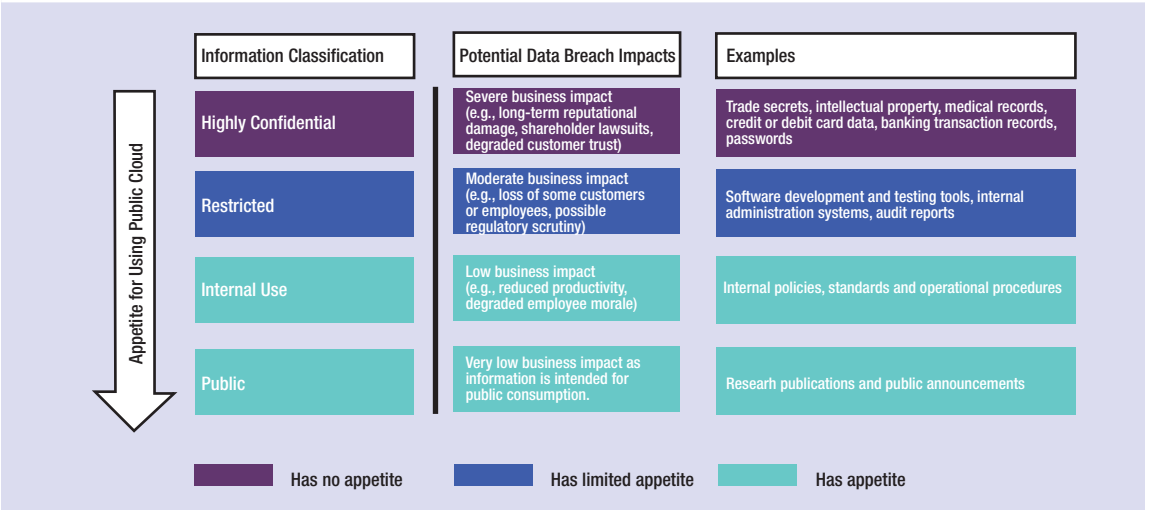
According to the CSA's September 2012 cloud encryption publication, *SecaaS Implementation Guidance, Category 8*,[9] encryption and protection of cryptographic keys are among the most effective data protection controls. High-value information should be encrypted when hosted in the cloud to minimise the risk of unauthorised disclosure. Robust key management is essential because losing encryption keys may result in data loss. The following recommendations should be considered when implementing encryption in the cloud:

- Implement tight controls to protect cryptographic keys, including a key life cycle management policy. NIST *Special Publication 800-57*[10] parts 1, 2 and 3 provide more detailed encryption key management guidelines.
- Ensure cloud encryption service includes disaster recovery and failover capabilities to minimise business impact if keys are lost.
- Define responsibilities for managing encryption keys. Retain key management to mitigate external breach of the service provider or malicious compromise by the service provider's privileged users.
- Test to confirm database encryption will not adversely impact application performance.
- Implement controls to purge data once removed from cloud storage.
- Complement data encryption with integrity protections such as digital signatures to maintain data authenticity.

### Deploy Strong Controls Over High-privileged Access

Managing privileged access is critical to securing data in the cloud. Privileged accounts remain an ideal attack vector for cybercriminals because they

**Figure 1—Information Classification for Cloud Adoption (Illustrative Example)**




**Source:** Phil Zongo. Reprinted with permission.

provide unlimited access to high-value applications and data. A CSA February 2016 publication, *The Treacherous Twelve: Cloud Computing Top Threats in 2016*,[11] identified account hijacking, usually with stolen credentials, as one of the top cloud security threats. The dynamic nature of cloud computing amplifies existing privileged user risk in a number of ways, including:

- Certain cloud access roles are extremely high risk and have the potential to shut down entire cloud environments.
- The shared responsibilities model implies that cloud service administrators may have privileged access to an organisation's infrastructure, applications or databases, depending on the service delivery model. This increases the attack surface.
- The speedy and seamless provision of new virtual servers rapidly introduces new privileged accounts to an environment. These accounts are often created with default passwords, which are an easy target for cybercriminals to exploit.
- Cloud administrators can provision new virtual server instances at the click of a button. If relevant authorisation is bypassed, this may result in unplanned expenses, undermining an organisation's cloud business case.

The following people, processes and technology controls can help reduce this exposure:

- Confirm the effectiveness of a cloud service provider's privileged access controls specifically hiring and oversight of system administrators.
- Implement strong passwords and automate security policy provisioning.
- Enforce two-factor authentication and two-person rule over high-impact activities.
- Log and monitor access to privileged accounts, including execution of high-impact commands.
- Retain superuser account credentials for accounts that give full access to all cloud resources.
- Regularly rotate passwords for service accounts, using an automated password management solution.

A number of cloud service providers have specific guidelines on how these controls can be implemented within their environments. For instance, the Amazon Web Services (AWS) Security Blog[12] provides detailed guidance for managing privileged accounts within AWS.

## Minimising Reliance on Cloud Service Providers

Improving service availability remains one of the key drivers for cloud adoption. Well-designed cloud solutions can significantly enhance business resilience as service providers continue to improve platform resiliency through clustering, replication and high-availability offerings.

In spite of these improvements, outages impacting multiple cloud service locations still occur. If not carefully planned for, these events may result in major supply chain and operational disruptions.

The good news is that reliable statistics are now available for businesses to assess cloud service reliability across different providers. For instance, Cloud Harmony, a third-party cloud vendor monitoring firm, provides independent comparison of cloud services based on service availability.

The following recommendations will help businesses mitigate these rare, but high-impact events:

- Review the cloud service provider's business continuity plan and disaster recovery plan to determine if they meet the organisation's recovery objectives.
- Utilise multiple cloud service providers to reduce risk of vendor lock-in.
- Implement high-availability cloud architecture to minimise service interruption.
- Complement the resilient architecture with regular backup and restore procedures, and store backup data outside of the cloud provider premises.
- Update and test the organisation's crisis management plan.



- Simulate recovery from different disaster scenarios, including recovery of individual applications, virtual environments and the entire cloud service provider.

From time to time, organisations terminate outsourcing arrangements—cloud arrangements are not an exception. Factors such as failure to meet performance requirements, security breaches or bankruptcy could lead to contract termination. To maintain business continuity and facilitate smooth transitions, organisations should formulate exit strategies or contingency plans to migrate critical records to an alternate solution, cloud or non-cloud.

## Conclusion

When properly planned, implemented and governed, the cloud can be a major catalyst for process improvement as well as a driver of business transformation. Cloud service providers are working relentlessly to improve their security and resilience capabilities. In reality, an organisation's onsite systems may not be more secure than the cloud. Security and reliability risk may not outweigh the lost opportunity to transform an enterprise with strategic use of the cloud. Cloud initiatives built upon enterprise strategy, coupled with robust risk management processes, have the potential to accelerate business innovation, transform customer experiences and improve competitive advantage.

## Acknowledgements

The author would like to thank Gina Francis, Innocent Ndoda, Kathleen Lo, Andrew Strong and Joe Chidwala for the valuable comments that helped improve this article.

## Endnotes

1 ISACA, *Innovation Insights: Top Digital Trends That Affect Strategy*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*
2 IDC, "Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC," USA, 21 January 2016, *www.idc.com/getdoc.jsp?containerId=prUS40960516*
3 Chan, W.; E. Leung; H. Pili; *Enterprise Risk Management for Cloud Computing*, Committee of Sponsoring Organizations of the Treadway Commission, June 2012, *www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf*
4 Australian Prudential Regulation Authority, *Outsourcing Involving Shared Computing Services (Including Cloud)*, 6 July 2015, *www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Outsourcing-Involving-Shared-Computing-Services.pdf*
5 The Economist Intelligence Unit, *Mapping the Cloud Maturity Curve*, IBM, 2015 *http://public.dhe.ibm.com/common/ssi/ecm/ku/en/kul12355usen/KUL12355USEN.PDF*
6 ENISA, *Cloud Computing—Benefits, Risks and Recommendations for Information Security,* Greece, December 2012, *https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security*
7 Humer, C.; J. Finkel; 'Your Medical Record Is Worth More to Hackers Than Your Credit Card', Reuters, 24 September 2014, *www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924*
8 Verizon, *State of the Market: Enterprise Cloud 2016*, 2016, *www.verizonenterprise.com/enterprise-cloud-report/*
9 Cloud Security Alliance, *SecaaS Implementation Guidance, Category 8: Encryption*, September 2012, *https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf*
10 National Institute of Standards and Technology, *Special Publication 800-57*, USA, *http://csrc.nist.gov/publications/PubsSPs.html#SP 800*
11 Cloud Security Alliance, *The Treacherous Twelve—Cloud Computing Top Threats in 2016*, USA, 2016, *https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf*
12 Amazon Web Services, AWS Official Blog, *http://aws.amazon.com/blogs/aws/*

# 2016GRC

an IIA and ISACA collaboration

Aug. 22–24, 2016 | Fort Lauderdale, Fla., USA

***The prior two GRC conferences sold out. Save your seat soon!***

Earn up to **18 CPE Credits.**
Register today at
**www.isaca.org/2016GRCIIA-jv4**.

# 5 TOP BENEFITS
## When You Attend GRC 2016

**There are many reasons to participate in GRC 2016. Here are five of the main advantages you can receive.**

1. Interact with world-class speakers, including keynotes Theresa Payton, former White House CIO, and Andrew Tarvin, International Humor Engineer.
2. Select from 48 thought-inspiring sessions to customize your learning needs.
3. Gain and share innovative ideas to solve your current and future business issues.
4. Build your global network of colleagues. The person sitting next to you just might hold the key to your next business breakthrough.
5. Earn up to 18 CPE hours, plus 7.5 more if you attend a pre-conference workshop.

**There is also a bonus benefit:**

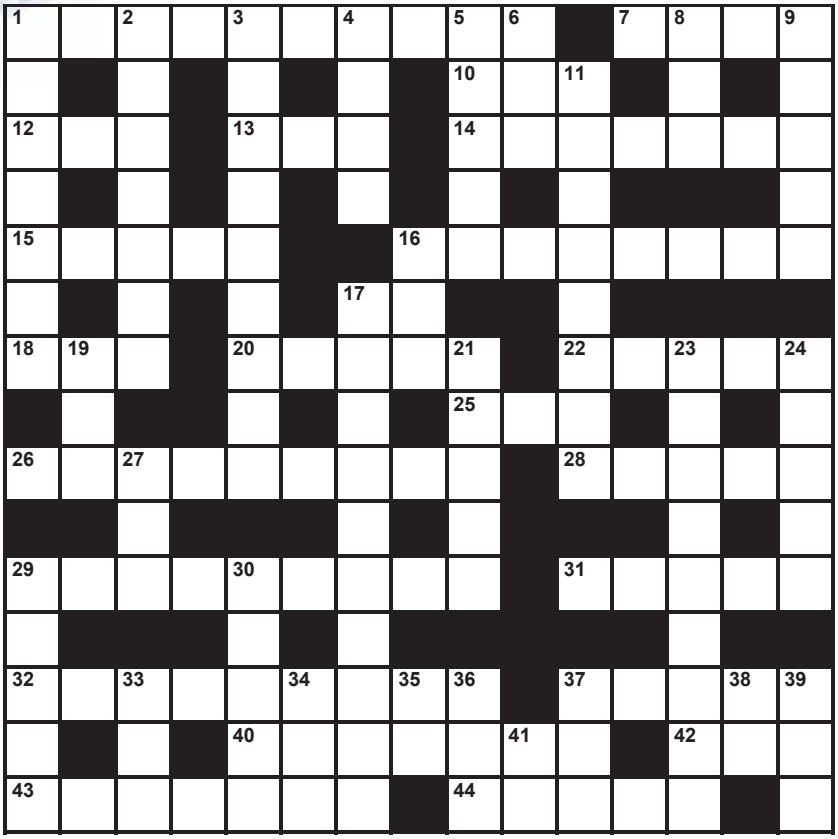
6. Enjoy business learning in a world-class setting with spectacular views of the Atlantic Ocean and the Intracoastal Waterway in South Florida.

The Institute of Internal Auditors

ISACA

# crossword puzzle

by Myles Mellor
www.themecrosswords.com



## ACROSS

**1** Type of encryption, 2 words
**7** Information security position, abbr.
**10** Cry of feigned innocence
**12** Berners-Lee invention
**13** Information unit, for short
**14** In IT, a reviewer of systems and processes
**15** It is usually found on a pad
**16** Strategy formers
**17** Memo start
**18** Highest degree
**20** Forestall, as in a cyberattack
**22** Suggestions, e.g.
**25** ___ behind the ears
**26** Part of a system
**28** Affirmatives
**29** Standard
**31** Stares conspicuously
**32** Critical point that when reached, may require changes of operation
**37** Word that goes with learning
**40** Revolution surfaces
**42** Investigate, with into
**43** Groups within groups
**44** Connection between things that are in a series

## DOWN

**1** Research institute monitoring information security, privacy and data protection
**2** Communicating with, 2 words
**3** Total amount
**4** On the cutting edge
**5** Communication medium used by hackers to penetrate computers and systems
**6** U in a text messsage
**8** World where physical objects are electronically linked, abbr.
**9** Evil monsters
**11** Cybercrime target
**16** For each one
**17** They control activities
**19** Driveway material
**21** Fine tune
**23** Access codes
**24** Tries out
**27** Have responsibility for
**29** Initial phases of a project
**30** Speed
**33** Steal
**34** Illegally obtained
**35** __-res file
**36** Noise
**37** Security exam
**38** Roman 6
**39** Urge, with on
**41** Germany's internet domain name

Answers on page 58

# quiz#167

Based on Volume 2, 2016—Project Management Methodologies and Associated Risk
Value: 1 Hour of CISA/CISM/CGEIT Continuing Professional Education (CPE) Credit

## TRUE OR FALSE

### ROSS ARTICLE

1 A true manager of risk should consider all aspects of the threats cyberattacks pose to an organization and devise approaches to transfer and control the hazards, accepting the rest in an informed manner.

2 Based on the products available in the marketplace to deal with cybersecurity, interest in recovery far outstrips those for prevention and detection.

### MORAN ARTICLE

3 It is incumbent on Agile risk management to address concerns such as recognition of threats and opportunities within a project, identification and prioritization of appropriate risk response strategies, and ability to judge whether or not risk is being managed.

4 One key difference between traditional and Agile project risk management is that ownership of risk is determined by project team members in a manner similar to the allocation of user stories and related tasks.

5 During risk assessment, the scores assigned to measure inherent risk cannot be used to construct a risk burndown chart, that does not track overall risk management efforts.

### EE ARTICLE

6 Despite a lesser amount of documentation, Agile can actually create greater transparency on uncertainties that may not be otherwise visible during a project's infancy.

7 Agile scenarios cannot force stakeholders to clarify just exactly what they need and cannot help to mitigate the risk of gold plating, which is the addition of features that do not add value. Thus, auditors cannot get involved early in the software development process by looking for comprehensive documentation upfront.

8 A key precept behind the emergence of design thinking as a means to solving problems is the emphasis on collaboration to attain sustainable product design.

9 Agile and Scrum are intended to be comprehensive. They address risk management, product strategy and other areas that comprise the slew of activities to enable and sustain product launch.

### MANI ARTICLE

10 Value analysis in Lean implementation involves assessing each process step through the eyes of the customer and determining whether the step is value-adding, nonvalue-adding or value-enabling activity.

11 The Kano model helps in visualizing work, reducing waste by limiting work in progress and maximizing customer value through a process known as value stream.

12 Many global IT business organizations have experienced a 30-50 percent increase in IT productivity and reduced the delivery time of new applications and functionalities/features by 20-40 percent through the application of Lean techniques such as value chain analysis.

### SHUBHAMANGALA ARTICLE

13 The cost of a data breach depends upon two factors: application criticality and corresponding sensitivity of data the application accesses.

14 Vulnerabilities are the basic reason for security attacks. They pose the greatest risk to application security.

15 Noncompliance costs organizations, on the average, 1.25 times more than meeting compliance rules. Because this cost is marginal, knowing the degree to which the application is compliant is optional.

CPE quiz

**Prepared by**
**Sally Chan,**
CGEIT, ACIS, CMA, CPA,

Take the quiz online

# CPE quiz #167

# THE ANSWER FORM

Based on Volume 2, 2016

## TRUE OR FALSE

### ROSS ARTICLE

1. _____

2. _____

### MORAN ARTICLE

3. _____

4. _____

5. _____

### EE ARTICLE

6. _____

7. _____

8. _____

9. _____

### MANI ARTICLE

10. _____

11. _____

12. _____

### SHUBHAMANGALA ARTICLE

13. _____

14. _____

15. _____

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CISM, CGEIT or CRISC # _____

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current *Journal* subscribers. An electronic version of the quiz is available at *www.isaca.org/cpequiz*; it is graded online and is available to all interested parties. If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to *info@isaca.org* or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA. Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address. You will be responsible for submitting your credit hours at year-end for CPE credits. A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.

**Answers: Crossword by Myles Mellor**

**See page 56 for the puzzle.**

# standards guidelines tools and techniques

## ISACA Member and Certification Holder Compliance

The specialised nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action.

## ITAF™, 3rd Edition

*(www.isaca.org/itaf)* provides a framework for multiple levels of guidance:

### IS Audit and Assurance Standards

The standards are divided into three categories:

- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

#### General
1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

#### Performance
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

#### Reporting
1401 Reporting
1402 Follow-up Activities

### IS Audit and Assurance Guidelines

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

Please note that the guidelines are effective 1 September 2014.

#### General
2001 Audit Charter
2002 Organisational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

#### Performance
2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of Other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

#### Reporting
2401 Reporting
2402 Follow-up Activities

### IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*.

An online glossary of terms used in ITAF is provided at *www.isaca.org/glossary*.

Prior to issuing any new Standard or Guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director of Privacy and Assurance Practices via email *(standards@isaca.org)*; fax (+1.847. 253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at *www.isaca.org/standards.*

**Disclaimer:** ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of these products will assure a successful outcome. The guidance should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IS environment.

*ISACA® Journal,* formerly *Information Systems Control Journal,* is published by the Information Systems Audit and Control Association® (ISACA®), a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal.*

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of the *Journal. ISACA Journal* does not attest to the originality of authors' content.



ISSN 1944-1967

**Subscription Rates:**

**US:**
one year (6 issues) $75.00

**All international orders:**
one year (6 issues) $90.00.

Remittance must be made in US funds.

# advertisers/ web sites



# leaders and supporters

ISACA®
Trust in, and value from, information systems

# ISACA BOOKSTORE

## RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

***www.isaca.org/bookstore***

CISA® CISM® CRISC™ CGEIT®

***COMING IN AUGUST!***

### CISA, CISM, CGEIT and CRISC Review Manuals Available as eBooks!

ISACA® Review Manuals in secure eBook format are compatible with any EPUB 3 reader such as Adobe Digital Editions or Bluefire Reader. These manuals will conveniently travel with you on your laptop, tablet or phone.

- Searchable content for greater ease-of-use
- Time-saving internal and external hyperlinks
- Interactive features within the table of contents
- Available for immediate download after purchase—with no waiting and no shipping cost anywhere in the world!

Browse over 450 publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***www.isaca.org/bookstore***

# FEATURED BOOKS

## Hacking Exposed Mobile Security Secrets and Solutions


by Joel Scambray, Jason Rouse, Neil Bergman, Mike Stanfield, Sarath Geethakumar, Swapnil Deshmukh, Scott Mats

**Product Code: 35MHEM**
Member/Nonmember: $40.00/$50.00

Identify and evade key threats across the expanding mobile risk landscape. *Hacking Exposed Mobile: Security Secrets & Solutions* covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems.

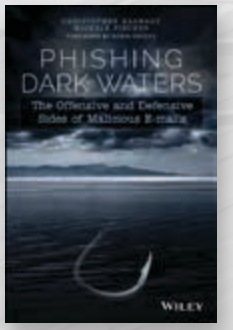
## Measuring and Managing Information Risk, 1st Edition


by Freund & Jones

**Product Code: 13EL**
Member/Nonmember: $40.00/$50.00

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, this book provides a proven and credible framework for understanding, measuring and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling and communicating risk within the organization, *Measuring and Managing Information Risk* helps managers made better business decisions by understanding their organizational risk.

## Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails




by Christopher Hadnagy, Michele Fincher, Robin Dreeke

**Product Code: 125WPD**
Member/Nonmember: $24.00/$34.00

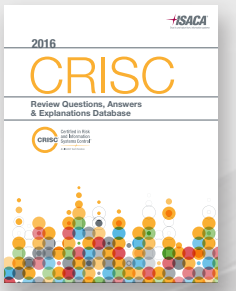
*Phishing Dark Waters* addresses the growing and continuing scourge of phishing emails, and provides actionable defensive techniques and tools to help you steer clear of malicious emails. Phishing is analyzed from the viewpoint of human decision-making and the impact of deliberate influence and manipulation on the recipient. With expert guidance, this book provides insight into the financial, corporate espionage, nation state, and identity theft goals of the attackers, and teaches you how to spot a spoofed e-mail or cloned website. Included are detailed examples of high profile breaches at Target, RSA, Coca Cola, and the AP, as well as an examination of sample scams including the Nigerian 419, financial themes, and post high-profile event attacks. Learn how to protect yourself and your organization using anti-phishing tools, and how to create your own phish to use as part of a security awareness program.

## 2 EASY WAYS TO ORDER:

**1. Online**—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore***

**2. Phone**—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

## CRISC Review Questions, Answers & Explanations Database—12 Month Subscription




by ISACA

**Product Code: XMXCR14-12M**
Member/Nonmember: $185.00/$225.00

The *CRISC Practice Question Database* is a comprehensive 500-question pool of items that contains the questions from the *CRISC Review Questions, Answers & Explanations Manual 4th Edition*. The database is available via the web, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity. The database is MAC and Windows compatible.

Exam candidates can take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing CRISC candidates to identify their strengths and weaknesses and focus their study efforts accordingly.

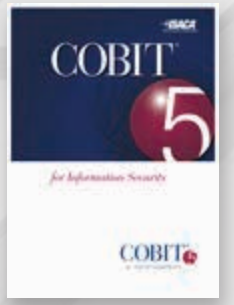
## Advanced Persistent Threats: How to Manage the Risk to Your Business


by ISACA

**Product Code: APT**
Member/Nonmember: $35.00/$60.00

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.

## COBIT 5 for Information Security




by ISACA

**Product Code: CB5IS**
Member/Nonmember: $35.00/$60.00

*COBIT 5 for Information Security* is a COBIT 5 Professional Guide. It examines COBIT 5 from a security view, placing a security lens over the concepts, enablers and principles within COBIT 5. Appendix B, Detailed Guidance: Processes Enabler is presented in the same format as the tables in *COBIT 5: Enabling Processes* and provides security-specific process goals and metrics, inputs/outputs, and activities.

*COBIT 5 for Information Security* is intended for all stakeholders in the enterprise because information security is the responsibility of all enterprise stakeholders. Using it can result in enterprise benefits such as improved risk decisions and cost management related to the information security function.

## Data Privacy for the Smart Grid


by Rebecca Herold, Christine Hertzog

**Product Code: 64CRC**
Member/Nonmember:
$70.00/$80.00

Many Smart Grid books include "privacy" in their title, but only touch on privacy, with most of the discussion focusing on cybersecurity. Filling this knowledge gap, *Data Privacy for the Smart Grid* provides a clear description of the Smart Grid ecosystem, presents practical guidance about its privacy risks, and details the actions required to protect data generated by Smart Grid technologies. It addresses privacy in electric, natural gas, and water grids and supplies two different perspectives of the topic—one from a Smart Grid expert and another from a privacy and information security expert.

## CSX Cybersecurity Fundamentals Study Guide


by ISACA

**Product Code: CSXG1**
Member/Nonmember:
$45.00/$55.00

The *Cybersecurity Fundamentals Study Guide* is a comprehensive study aid that will help to prepare learners for the Cybersecurity Fundamentals Certificate exam. By passing the exam and agreeing to adhere to ISACA's Code of Ethics, candidates will earn the Cybersecurity Fundamentals Certificate, a knowledge-based certificate that was developed to address the growing demand for skilled cybersecurity professionals. The *Cybersecurity Fundamentals Study Guide* covers key areas that will be tested on the exam, including: cybersecurity concepts, security architecture principles, incident response, security of networks, systems, applications, and data, and security implications of evolving technology.

## Implementing the NIST Cybersecurity Framework


by ISACA

**Product Code: CSNIST**
Member/Nonmember:
$35.00/$60.00

In 2013, US President Obama issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, which called for the development of a voluntary risk-based cybersecurity framework (CSF) that is "prioritized, flexible, repeatable, performance-based, and cost-effective." The CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). ISACA participated in the CSF's development and helped embed key principles from the COBIT framework into the industry-led effort. As part of the knowledge, tools and guidance provided by CSX, ISACA has developed this guide for implementing the *NIST Framework for Improving Critical Infrastructure Cybersecurity.*

## 2 EASY WAYS TO ORDER:

**1. Online**—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore***

**2. Phone**—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

# CYBER STRONG.

Claim your future in the high demand Cybersecurity and information assurance/security fields. Students will be educated in the technical aspects of Cybersecurity systems and will be prepared for the management, operations and oversight of these systems.

***Classes are forming now in our state-of-the-art Cybersecurity laboratory and online.***

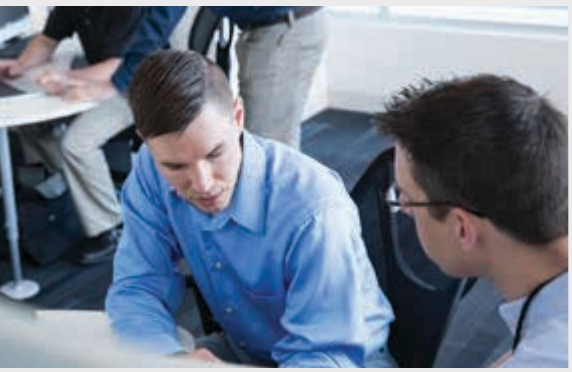
SAINT LEO UNIVERSITY®

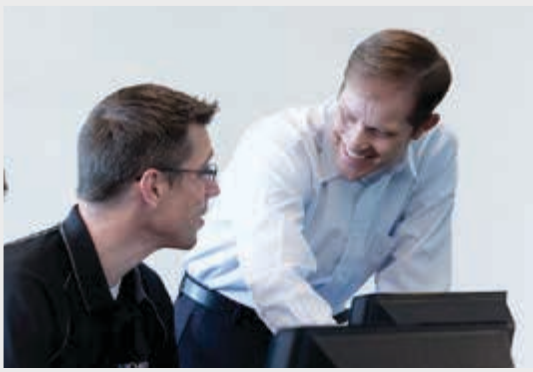
**Saint Leo University offers competitive degree programs designed to train students in the field of cybersecurity.**
**B.S. Computer Science - Information Assurance**
**B.S. Cybersecurity**
**M.S. Cybersecurity**

## 800.707.8846 | SaintLeo.edu

National Security Agency and the Department of Homeland Security have designated Saint Leo University as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through academic year 2021.

# TRAIN LIKE YOU FIGHT





## CHIRON'S TEAM OF EXPERT INSTRUCTORS BRING YEARS OF RELEVANT, REAL-WORLD EXPERIENCE INTO THE CLASSROOM.

Chiron's cyber protection program trainees are challenged and tested with real-world scenarios based on today's dynamic, agile and constantly evolving threat environment. Unlike simulated training, Chiron's classes are held in a laboratory setting unrestricted by rigid network security constraints that hamper the hands-on learning experience.

Our customized training approach creates qualified Information Operations professionals that are tested and equipped to handle the real-life cyber threats of today.

- OFFENSIVE AND DEFENSIVE CYBER OPERATIONS
- ADVANCED THREAT SIMULATION
- NETWORK FORENSICS AND THREAT ANALYSIS
- MALWARE REVERSE ENGINEERING
- SIMULATED TRAINING ENVIRONMENT

LEARN MORE ABOUT OUR TRAINING:

410-672-1522, ext. 113 | training@chirontech.com

or visit chirontech.com

CHIRON