THE SMART TRANSFORMATION

HEALTHCARE SECURITY—THREE PARADOXES AND THE NEED FOR A PARADIGM SHIFT

CYBERSECURITY VS. MASTER DATA MANAGEMENT

SECURE ELECTIONS IN A SMART WORLD
Prepare to Be the One Changing the Future of IT and Business with Keynote and Innovator Luke Williams


See the world through the eyes of opening keynote speaker and authority on disruptive innovation Luke Williams.

Embrace his thinking and you may never look at information systems governance, risk, and control—nor your business and role in it—the same again.

Register Soon—space is limited and previous events have sold out.

www.isaca.org/GRC18-jv3

SAVE US$200 WHEN YOU REGISTER BY JUNE 18, 2018! | EARN UP TO 18 CPE HOURS.
The Society of Corporate Compliance and Ethics International Basic Compliance & Ethics Academies® provide three and a half days of classroom-style training in the fundamentals of compliance and ethics management. Learn everything from understanding risk, and setting policies, to training and investigations.

Topics addressed at an academy include:
- Standards, policies, and procedures
- Compliance and ethics program administration
- Communications, education, and training
- Monitoring, auditing, and internal reporting systems
- Response and investigation, discipline and incentives
- Anti-Corruption and Bribery
- Trade Sanctions
- Risk assessment

corporatecompliance.org/academies

Questions: lizza.catalano@corporatecompliance.org
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.

Letter From the Editor: From Print to Digital—The Journal Transformation
Jen Hajigeorgiou, Editor

Information Security Matters: Security in the Migration to a Multi-Modal Environment
Steven J. Ross, CISA, CISSP, MBCP

IS Audit Basics: Auditing Data Privacy
Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt

The Network
Lucio Augusto Molina Focazzio, CISA, CRISC, CISM, COBIT Assessor and Trainer, ITIL

FEATURES

Clash of the Titans
( Também disponível em português)
Ofir Eitan, CISM, CCSK, CTI

Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift
Giuliano Pozza, CGEIT, e-CF Plus (CIO), ITIL v3

Cybersecurity vs. Master Data Management
( Também disponível em português)
Chip Jarnagin, CISSP, CSM, PMP, and Sonja Hammond, CISSP, ITIL Foundation, PCI-ISA

Secure Elections in a Smart World
Ed Moyle

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 2018.

Building a Strong Security Posture Begins With Assessment
Tyler Hardison, CISSP, QSA

Merging Internal Audit Departments
Kevin Alvero, CFE, Randy Pierson, CISA, and Wade Cassels, CISA, CIA, CFE, CRMA

IT Risk Management Based on COBIT 5 for Risk at Deutsche Telekom AG
Horst Moll, CISA, CRISC, CISM, CCSE, CISSP, ISO 27001 LA, MBCI, MCP

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.
From Print to Digital—The Journal Transformation

As technology continues to transform the way people consume information, the work of ISACA’s professional community becomes more important—and challenging. The ISACA® Journal has a proud tradition of serving our community for more than 40 years, evolving to meet the needs and interests of practitioners amid the ever-changing technology landscape.

The Journal remains committed to connecting you and the entire ISACA® professional community with valuable content and delivering it in the format that readers most desire in the digital era. In recognition of how more and more professionals consume information today, we are refocusing the way we deliver the ISACA Journal with added emphasis on our digital presence, allowing this valuable knowledge resource to better serve our professional community and help us move more quickly toward the goal of realizing the positive potential of technology.

Effective with volume 4, 2018, of the ISACA Journal (July/August edition), you will receive ISACA Journal content exclusively in a digital format unless you choose to opt in to receive the print edition. If you wish to continue receiving the print edition, you must opt in by 26 June 2018 to ensure uninterrupted delivery. To do so, follow these simple steps:

- Log into the myISACA section of the ISACA website
- Click on the myProfile tab, selecting the Account-Address-Demographic tab
- Click Edit and select the My Demographic and Other Information tab
- Check the box to opt in under the ISACA Journal Delivery Options—Print and/or Digital section.

By accessing the Journal online, you and other members of ISACA’s professional community can explore the Journal alongside ISACA’s broad range of online knowledge resources. You can build on your understanding through ISACA white papers, audit and assurance programs, blog content and more, and gain further insights from our network of affiliates, which includes the Massachusetts Institute of Technology Center for Information Systems Research and Wapack Labs.

To continue uninterrupted delivery of the print edition of the ISACA Journal, opt in by 26 June 2018.

- Log into the myISACA section of the ISACA website
- Click on the myProfile tab, selecting the Account-Address-Demographic tab
- Click edit and select the My Demographic and Other Information tab
- Check the box to opt in under the ISACA Journal delivery options—Print and/or Digital section.

No matter how or where you consume Journal content, we are committed to providing the knowledge resources you need to navigate digital disruption and gain actionable industry insights. Thank you for reading and enjoy the latest edition of the Journal!

Sincerely,

Jen Hajigeorgiou
Editor
The Importance of Planning

The most important factor in any successful voyage is knowing where you are going. In the migration to a multi-modal environment, this implies detailed and well-documented planning. The documentation is especially important, because the journey will likely be a long and arduous one; there will be some who leave it and others who join in the middle. It is all well and good to know where you are going, but a good road map is always helpful. And it is on the basis of this plan and its documentation that (information) security along the route will be determined.

A common mistake I have observed with some information security professionals is to stomp their feet, hold their breath and cry, “I’m not going” and, by implication, neither are you. It is not an original observation, but change is difficult. The current environment may be familiar and there may have been considerable investment in securing both the physical and logical infrastructure, but the combination of financial, technical and environmental pressures is making this transition inevitable. Standing in the way only demeans information security; it is seen as a roadblock and it does nothing to improve the eventual quality of security.

Information Security and IT Operations

It is far more valuable for the information security function to be a part of the planning process, in close alignment with IT operations. Information security makes policy, and operations implements it. With the move to multi-modalism, both are facing significant transformation in their job functions. They are both moving from *doing* things to *making sure* that third parties do those things. In effect, both security and IT operations are transitioning to vendor management functions. They have a shared stake at this point in the migration to ensure that the vendors make things go right. (And so, not really by the way, does IT audit.)
Of course, this is not a new experience; organizations have been choosing to use SaaS for decades, even if they did not call it SaaS. The difference is that the applications moving out of the data center are increasingly at the core of the mission of the organization. For just one example, SAP is, for many organizations, their most critical application. The company is committed to supporting in-house versions of its widely adopted software until 2025, but not thereafter. SAP users are confronting the move to the cloud in their strategic planning today. It is time now to consider how critical applications and data will be protected once they are running on someone else’s computers in someone else’s data center. Attention must also be given to how they will be protected while this move is occurring.

Security En Route

It is almost impossible to move all of an organization’s applications at once. For one thing, they will not all be going to the same places the same way. For example, some may be transferred to the cloud, but remain essentially unchanged otherwise. Others may be replaced by superior vendor-derived applications. Some may be “lifted and shifted” to a colo facility, and possibly into the cloud thereafter. Assuring that only authorized users access only the applications and data they are authorized to use—and that unauthorized people and systems do not—is challenging enough in a relatively stable environment. It is well-nigh impossible when the hardware, software, network and physical locations of the applications and data in question change from day to day.

The solution is to focus on the process. If security professionals think of the gestalt of the information, the applications that manipulate it and the infrastructure that supports it, rather than its constituent parts (admittedly, a difficult task), securing the migration to multi-modalism becomes comprehensible, if not easy. Nobody ever thought it would be easy, but this era of information technology may offer a once-in-a-generation opportunity to rethink the architecture of security.

Trust No One

One thing that can be said for proprietary data centers and the hardware and software in them: We knew who had the ability to enter and touch the physical manifestations of information technology. We had a basis for establishing trust in those people. In multi-modal environments we do not know who or what can go where, so trust no one. Every person and the systems they use—their domains—must be discretely tied to the applications and data they are allowed to use. Each individual must present those credentials before using the resources. The credentials themselves must be protected with public key cryptosystems. Movement from domain to domain must require a return to a checkpoint for credentials to be revalidated.

All of this security must be built into the environment. The last time there was a shift of this magnitude in the way information technology was organized occurred when we moved from massive centralization—mainframes—to distributed
processing. Candidly, we security professionals did not manage that one well. In fairness, there was not the perception of the need for security on the part of the vendors that there is today. A security architecture something like the one I described above needs to be a part of the selection criteria for multi-modal services.

It took a decade or more to get back to the level of security that centralization offered. The advent of viruses, distributed denial-of-service (DDoS) attacks and data leakage has underscored that failure. It remains to be seen whether we will do better this time.

Author’s Note

I very much enjoy hearing from readers of this column, either with criticism (which makes me better) or praise (which makes me smile). Some choose to email me, which is great, and others use the Comments section of the online ISACA® Journal, which is also great. If you do write a Comment online, I urge you to check back later. I always read your comments and I always reply.

Endnotes

2 Applications running on cloud technology are SaaS, but not all SaaS applications are in the cloud. Some are simply accessed over the Internet, without the multi-center concurrency of true cloud technology.
5 Some may say that the era of portable devices is an equally great transformation. From the individual’s standpoint, that is so. But for the management of organizations and governments, I do not see it that way. No organization I know is running general ledger on a smartphone.
Auditing Data Privacy

I consider myself a private person, so, naturally, this tendency is reflected in my online profile. I do have Facebook and Instagram accounts, but these were initially created to monitor my children’s online activity and I rarely, if ever, post on them. I also have Twitter and LinkedIn accounts, which I use to post technology-, audit- and cybersecurity-related news. My only real online presence is reflected in this column, related blogs and anything ISACA® posts to promote same.

So, is my privacy maintained? With the advent of machine learning, it is possible to classify text in any number of ways. Web services1 exist that use labeled training texts to determine the mood, gender, age and personality2 of content authors. I have fed some of my previous columns into the site and some of the classifications are scarily accurate.

Privacy is the right of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context and according to the purposes for which it was collected or derived.3 The context is important. I am aware that this column is posted online and does not require a password to access, therefore, I cannot reasonably expect my privacy to be fully maintained.

However, now consider your last audit report. How would you feel if it was used to classify your personality? Could your next promotion be decided by artificial intelligence (AI)? Is this acceptable? Probably not without consent. So how can we audit to help mitigate this and other privacy risk?

In previous columns,4 5 I advocated the use of an ISACA paper on creating audit programs.6 This article will once again apply this process to build an audit program for privacy for your organization.

Determine Audit Subject

The first thing to establish is the audit subject. What does privacy mean in your enterprise? If there are distinct categories of data in use for different areas of the business, they should probably be recorded as separate audit universe items. Fundamentally, though, when considering privacy, the data can be broken down to data stored on customers and employees (the right of an individual).7 Besides databases, files and documents, it is important to also consider where the data are stored and/or from where they are derived, including.8

• Social media
• Cloud computing
• Mobile devices
• Big data analytics/machine learning/AI
• Internet of Things (IoT)
• Personal devices (bring your own device [BYOD])
• Tracking/surveillance technologies—drones, radio frequency identification (RFID) tags, closed circuit television (CCTV), global positioning satellite (GPS) devices

The key is to consider categories of data and determine the audit subject(s). You need to answer the key question: What are you auditing?

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA committees and is a current member of ISACA’s CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke supported the update of the CISA® Review Manual for the 2016 job practices and was a subject matter expert for ISACA’s CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (ian_I_Cooke@hotmail.com), Twitter (@COOKEI), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.
Define Audit Objective

Once you have decided what you are auditing, you need to establish the objective of the audit. Why are you auditing it? From an auditor’s perspective, it is advisable to adopt a risk-based view and define the objectives accordingly:

- First, consider the seven categories of privacy:
  1. Privacy of person
  2. Privacy of behavior and action
  3. Privacy of communication
  4. Privacy of data and image (information)
  5. Privacy of thoughts and feelings
  6. Privacy of location and space (territorial)
  7. Privacy of association

- Next, consider the risk across the seven categories (figure 1). Privacy risk can lead to adverse publicity and reputational damage resulting in customer and economic loss, including fines.

Set Audit Scope

When you have defined the objectives of the audit, you should use a scoping process to identify the actual data that need to be audited. In other words, what are the limits to the audit? This could include data in a specific application, process, location or stored by certain devices. Again, this should be risk based.

Perform Pre-Audit Planning

Now that you have identified the risk, it should be evaluated to determine its significance. Conducting a risk assessment is critical in setting the final scope of a risk-based audit. The more significant the risk, the greater the need for assurance. Sample assurance considerations based upon the privacy principles include:

<table>
<thead>
<tr>
<th>Privacy Category</th>
<th>Example Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy of behavior and action</td>
<td><strong>Social media</strong> contains information, images, video and audio that reveal personal activities, orientations and preferences, many of which are sensitive in nature and can impact the data subjects.</td>
</tr>
<tr>
<td>Privacy of thoughts and feelings</td>
<td><strong>Big data analytics</strong> has the potential to take large amounts of data and reveal the thoughts or feelings of specific individuals based on data they provide or others provide about them. Such insights can result in negative impact if actions are taken because of the analytics findings.</td>
</tr>
<tr>
<td>Privacy of location and space (territorial)</td>
<td><strong>Privately owned computing devices</strong> that are used for business activities may also be able to record images and audio. Such images and audio create privacy risk if the devices are also used to perform business activities within the workplace.</td>
</tr>
</tbody>
</table>

• Choice and consent—Does the enterprise ensure that appropriate consent has been obtained prior to the transfer of personal information to other jurisdictions?

• Legitimate purpose specification and use limitation—Does the enterprise specify the purpose(s) for which personal information is collected?

• Personal information and sensitive information life cycle—Does the enterprise retain personal information for only as long as necessary?

• Accuracy and quality—Does the enterprise implement practices and processes to ensure that personal information is accurate, complete and up to date?

• Openness, transparency and notice—Does the enterprise provide clear and easily accessible information about its privacy policies and practices?

• Individual participation—Does the enterprise provide data subjects a process to access their personal information?

• Accountability—Does the enterprise assign roles, responsibility, accountability and authority for performing privacy processes?

• Security safeguards—Does the enterprise ensure that appropriate security safeguards are in place for all personal information?

• Monitoring, measuring and reporting—Does the enterprise report compliance with policies, standards and laws?

• Preventing harm—Does the enterprise establish processes to mitigate any personal harms that may occur to data subjects?

• Third-party/vendor management—Does the enterprise implement governance processes to ensure the appropriate protections and use of personal information that are transferred to third parties?

• Breach management—Has the enterprise established a documented policy and supporting procedure for identifying, escalating and reporting incidents?

• Security and privacy by design—Does the enterprise ensure executive support for the identification of personal information and privacy risk within enterprise events?

• Free flow of information and legitimate restriction—Does the enterprise follow the requirements of applicable data protection
select the audit approach or strategy and start developing the audit program. You now have enough information to decide what documents you expect to see, what laws and regulations apply, the criteria, and whom you are going to interview. You do, however, need to define the testing steps.

In the latter half of 2017, ISACA released an audit/assurance program that defines testing steps for data privacy. As always, this should be considered a starting point and should be adjusted based upon risk and criteria that are relevant to the organization you are auditing. It is worth spending the time to consider the risk and the resulting need for assurance (figure 3).

Key testing steps in the audit program are security related. However, it is important to remember that security does not mean privacy. Confidentiality is preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information. Privacy is a possible outcome of security.

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and authorities for the transfer of personal information across country borders?

Interviewing the auditee to inquire about activities or areas of concern that should be included in the scope of the engagement. Once the subject, objective and scope are defined, the audit team can identify the resources that will be needed to perform the audit work.

“IT IS IMPORTANT TO REMEMBER THAT SECURITY DOES NOT MEAN PRIVACY.”

Determine Audit Procedures and Steps for Data Gathering

Figure 3—Assurance Consideration to Audit Program Mapping

<table>
<thead>
<tr>
<th>Privacy Principle Number</th>
<th>Audit Program Sample Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>When personally identifiable information (PII) is obtained from individuals, consent is obtained.</td>
</tr>
<tr>
<td>2</td>
<td>Clear guidelines are in place to ensure the appropriate use and retention of data throughout the enterprise.</td>
</tr>
<tr>
<td>3</td>
<td>Clear guidelines are in place to ensure the appropriate use and retention of data throughout the enterprise.</td>
</tr>
<tr>
<td>4</td>
<td>Determine if the record management guideline describes the enterprise’s strategy and procedures regarding maintenance, retention and destruction of records in accordance with all state and federal laws and regulations.</td>
</tr>
<tr>
<td>5</td>
<td>When PII is obtained from individuals, consent is obtained.</td>
</tr>
<tr>
<td>6</td>
<td>Purpose and scope/applicability of the record management process are clearly defined.</td>
</tr>
<tr>
<td>7</td>
<td>Roles and responsibilities of the people involved in the management of data governance for privacy, confidentiality and compliance for the enterprise have been clearly defined.</td>
</tr>
<tr>
<td>8</td>
<td>Appropriate data encryption standards are in place for data at rest, and appropriate awareness campaigns are conducted to train employees.</td>
</tr>
<tr>
<td>9</td>
<td>Awareness is accounted for and key metrics are utilized for conformance and compliance to required training.</td>
</tr>
<tr>
<td>10</td>
<td>Integration of privacy impact assessments (PIAs) is firmly established in the enterprise and proper tools and monitoring are in place for the validation of compliance.</td>
</tr>
<tr>
<td>11</td>
<td>Contractual language for third-party management of PII is appropriately included and agreed upon.</td>
</tr>
<tr>
<td>12</td>
<td>The breach escalation plan is in place to react to PII breaches.</td>
</tr>
<tr>
<td>13</td>
<td>Data deidentification across the enterprise is enforced appropriately through tools and automated means.</td>
</tr>
<tr>
<td>14</td>
<td>Global privacy policies and requirements have been modified to align with region- or country-specific requirements.</td>
</tr>
</tbody>
</table>
Conclusion

New and emerging technologies will enable enterprises to derive increased insight and, thus, value from data. This will, no doubt, provide competitive advantage. ISACA’s Privacy Principles can be used as an overarching framework in conjunction with these technologies to provide assurance that an enterprise respects the privacy rights of an individual. Demonstrating this to those individuals will also provide a competitive advantage.

Endnotes

1 uClassify is a free machine learning web service. https://www.uclassify.com/
7 Op cit ISACA, ISACA Privacy Principles and Program Management Guide, p.11
8 Ibid. p. 31
9 Ibid. p. 28
10 Ibid. p. 31
15 Op cit ISACA, ISACA Privacy Principles and Program Management Guide, p. 44
17 Ibid.
20 Ibid.
Q. How do you think the role of the IS audit professional is changing or has changed?

A. Over time, the role of the IS audit professional has been changing due to advances in technology and the sophistication of risk and controls. From evaluating controls around the computer, the IS audit professional went on to evaluate the computer itself. Now, as technology evolves, audits are focused on evaluating computational environments such as the cloud; artificial intelligence; and specialized topics related to cybersecurity and information security, including the evaluation of third parties within audit scope.

This evolution has resulted in the IS audit professional knowing and specializing in industry standards (e.g., International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] 27001 and ISO/IEC 22301), good practices (ITIL), and reference frameworks such as COBIT® 5 and The Open Group Architecture Framework (TOGAF), as well as specializing in computational tools.

Q. What leadership skills do you feel are critical for professionals to be successful in the field of IS audit?

A. They should be advisors to the executive level, providing critical thinking and analysis. In addition to their skills that detect and identify risk, IS audit professionals should be able to motivate their clients to improve their culture through controls. They should be good communicators, able to write effective audit reports and “sell” them. They must also have the ability to analyze and solve problems to make recommendations that provide value to the organization, remembering the need to reinvent and innovate themselves continuously.

Q. What is the best way for someone to develop those skills?

A. Being a leader is not giving orders; it is teaching by example. Leaders always do more than what is asked of them and they guide their subordinates toward success. Leadership is learned through practice; having a coach makes it much better. Attitude is also very important. Leaders must be able to detect weaknesses and strengths in their team, to overcome the weaknesses and take advantage of the strengths.

Q. What advice do you have for IS audit professionals as they plan their career paths and look at the future of information security?

A. In this digital world, modern IS audit professionals have the evaluation of cybersecurity and information security among their main activities. To do this, they must strengthen their knowledge on the subject; they must know the information security standards and the risk and vulnerabilities of the information and the platforms on which the information resides. Using this knowledge in the development of audits will allow them to apply global knowledge about the security risk of business information and, at the same time, a more detailed knowledge of the areas related to information security. I would advise IS audit professionals to earn the Certified Information Systems Auditor® (CISA®) certification because it is globally recognized. It is also highly desirable for IS audit professionals who wish to function at a management level.
to earn the Certified Information Security Manager® (CISM®) credential. Those who prefer a more technical perspective should pursue the Certified Information Systems Security Professional (CISSP) credential.

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. My ISACA® certifications have changed my life. They opened a very wide professional field to me. As soon as I earned my Certified Information Systems Auditor® (CISA®), I was promoted in the organization where I worked. When I added the CISM and the Certified in Risk and Information Systems Control™ (CRISC™) certifications, I was able to be more competitive in the field of consulting because organizations look for certified professionals. Certifications show that the person has the experience and knowledge required to perform the needed function. Private companies and the government usually give additional points in their competitive bids and tenders when the team vying for the assignment has international certifications. In the environment I work, ISACA certifications are highly desired, so I always hope that the resources I hire have earned one or more of the ISACA professional certifications and that they are also certified in COBIT 5, preferably as implementers or assessors.

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

A. Every day, new regulations appear that force organizations to evaluate their risk and improve their controls. Additionally, IT governance in organizations is increasingly in demand. Therefore, I think that the role of the IS auditor related to governance and compliance will be increasingly important, and IS auditors should evolve toward expanding their audit spectrum by supporting their organizations in achieving implementation and maintenance of IT governance and complying with local laws and regulations as well as those of other countries (such as the US Sarbanes-Oxley Act [SOX]).

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

A. My work life has been full of challenges, but I think one of the most difficult was when a consulting company asked me to join its team of professionals to help Ecopetrol, the largest oil company in Colombia, comply with SOX, supported by COBIT. This is work that should be done in a short period of time. Thanks to the support of top management and the excellent teams from both Ecopetrol and the consulting company, we achieved the goal. My role was serving as the COBIT expert and my mission was to help Ecopetrol understand the benefits of applying COBIT and how to integrate it with other international practices and standards to comply with SOX.

I had to work with different areas of the company to improve their knowledge about the use and application of COBIT. I held talks at all levels on COBIT, trained the staff on COBIT, and coached the team on the integration of COBIT with other international standards and practices.

1. What is the biggest security challenge that will be faced in 2018? How should it be addressed?

Identifying, containing and responding to targeted information attacks, especially phishing and ransomware. To respond, increase management awareness, strengthen regulations, train company personnel on information security, and strengthen the IT security infrastructure with predictive tools and artificial intelligence.

2. What are your three goals for 2018?

- Earn the Cybersecurity Fundamentals Certificate.
- Triple the number of COBIT Implementation and Assessor courses I present.
- Make my farm start producing.

3. What is your favorite blog?

ITInsecurity (insecurityit.blogspot)

4. What is on your desk right now?

- My new Surface computer
- COBIT 5 books (COBIT® 5: Enabling Processes, COBIT Process Assessment Model (PAM): Using COBIT® 5, COBIT® 5 for Assurance)
- A glass of tea

5. How has social media impacted you professionally?

Social media is an excellent way to share knowledge and sell services. I take advantage of social media to know people around the world with similar interests. I can increase my knowledge and sometimes I can help people by answering different kinds of concerns about the profession.

6. What is your number-one piece of advice for other IS audit professionals?

To study, learn, and practice, practice, practice continuously. Our profession is like the medical profession; everything is continually changing and must keep up with the change.

7. What is your favorite benefit of your ISACA membership?

To access to the knowledge base to learn, and the ISACA® Journal

8. What do you do when you are not at work?

I walk and play with my Catahoula leopard dog.
Clash of the Titans
How to Win the “Battle” Between Information Security and IT Without Losing Anyone

Ofir Eitan, CISM, CCSK, CTI
Is a cybersecurity manager and consultant with more than 10 years of managerial experience in various fields, including strategy and road mapping, security programs, vendor management, product evaluation, incident response, threat intelligence, and offensive security. He established the first cybersecurity team in Leumi Card, the second largest payment company in Israel. Prior to that, he served in the Israeli National Cyber Bureau and the Israeli Intelligence Corps in various positions as an information security officer and cyberthreat intelligence (CTI) team leader. He can be reached at www.linkedin.com/in/ofir-eitan.

One of the major challenges chief information security officers (CISOs) face in almost any organization is prioritizing information security interests with regard to IT interests. Examples include implementing a cybersecurity system before implementing a system designated for better network performance or changing the network architecture based on security directives rather than designing it in a way that will be easier to maintain by the IT operations teams. Any reader who has experienced working in an IT division has probably encountered the following common dilemma: The CISO presents an urgent need to acquire a security system and the IT department has to oppose the request due to insufficient resources or technical issues derived from the project.

This article shares the author’s insights from his personal experience regarding the imminent and almost inevitable clash between information security and IT interests. These thoughts developed while the author participated in related roundtables, took part in corporate meetings on this topic, and also partook in informal conversations with experts and senior executives in the industry. This analysis can help information security officers and managers overcome this challenge and help organizations to leverage their security posture.

The dynamic in the workplace is generally based on workers and their interaction with one another. Therefore, a good working relationship between CISOs and their colleagues, such as the head of the system operations department, would likely have a positive impact on bridging their professional individual interests. On the other hand, the location of the information security functions in the organizational structure can have a huge impact on the working dynamic, as indicated (based on the author’s preferred comprehension of the evolution of the information security structure):

• The CISO reports to the head of the IT department or an equivalent position—In many organizations, specifically small to medium-sized businesses (SMBs), security functions have developed inside IT units, mainly to meet the demand for securing IT, based on a true understanding of the increase in cyberthreats or to ensure compliance with regulatory demands. Although a proper security posture can always be achieved, in this scenario, conflicts may arise due the potential intrinsic conflicts of interest between performance needs and security needs. For this main reason, best practices and standards require the separation of duties between IS and IT.

Também disponível em português
www.isaca.org/currentissue

Do you have something to say about this article?
Visit the Journal pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts. https://bit.ly/2Gi6I2q
• The CISO reports to the chief information officer (CIO) but relies on IT units for system operations and management—This structure tends to be common among corporate entities. Usually, this model separates management of security policies, audit and monitoring incidents led by the information security unit from the infrastructure and/or system units, which are executing system operations. Therefore, the CISO generally relies on the infrastructure department when it comes to budget and is coerced to toe the line with the CIO’s inherent interests, which usually lean toward IT productivity. Once more, pressure from business units, performance issues, and insufficient human or financial resources can be placed before the CISO’s agenda.

• The CISO reports to a senior executive, but not the CIO—Most organizations today are obligated to comply with industrial regulations, which seem to move toward the direction of requiring organizations to place the CISO in a position of reporting to a senior executive. In this case, the CISO can report to the chief risk officer (CRO), chief operating officer (COO) or other senior positions. Any of those structures may, or may not, have negative effects on the CISO’s ability to promote information security interests in the IT division. However, the CISO’s relative distance from the IT units can impose the biggest challenge to his/her duty, whether in budgetary manners, staying up to date with IT projects and trends, or enforcing policies and promoting the IS agenda.

• The CISO manages independent system operators and reports to the CIO or chief executive officer (CEO)—Some might say this structure is the goal for any CISO since it provides the necessary resources and authority to execute information security governance and the associated agenda. As the saying goes, with great power comes great responsibility, therefore, in this structure, the CISO will likely be required to invest more time coordinating system operations with the IT units. The key factor in this structure is to assimilate the information security system operators with their colleagues in the IT units to join forces on a daily basis.

In the author’s point of view, there is no ideal model for placing the CISO in any given organization. On the contrary, there is always a best model for any specific organization. One way or the other, it is advised that CISOs absorb the idea that their place in the organization’s layout has a vital influence on their ability to lead major changes such as acquiring new solutions, implementing a new and secured network architecture, and executing comprehensive policies and processes.

The organizational structure analysis should come in handy for any CISO as a means to understand the pros and cons of the position. However, the following insights and guidance may apply for the CISO no matter the reporting lines in the organizational structure layout:

“IT IS RECOMMENDED THAT THE CISO FORMALIZE AN OPENING TERMS DOCUMENT WITH ALL THE BASIC DEMANDS SET BY THE IT DEPARTMENTS.”

• Understand and consider both sides of the equation. Naturally, information security personnel pursue solutions with the best security functionalities and capabilities according to their informed understanding. On the other hand, each information security manager should consider whether the solution meets the demands of the infrastructure, system and IT operations units. It is recommended that the CISO formalize an opening terms document with all the basic demands set by the IT departments. This solution is comparable to security policies, but from an IT point of view (e.g., an agent or agentless system, the support of virtual desktop infrastructure [VDI] platforms, the system resource limits, sufficient technical support). Both information security and IT units should aspire for a harmonious process in which each side represents the other’s needs and interests.

• Remember that business needs will always be placed above IS needs. When it comes to the bottom line, managing information security...
means finding the best compromise between security and business for the organization while ensuring compliance with laws and regulations. For that reason, this understanding also applies to the considerations behind purchasing and implementing new security systems. Therefore, before presenting a business case, the CISO must make sure purchasing new solutions or changing the network architecture is the last resort and all other solutions based on existing resources were properly considered.

• Develop a business case. Finding the financial and human resources for the best security solution in the market is often not enough if there is no tangible, concrete or imminent risk. Therefore, prioritizing security needs over business needs may require the CISO to find other sources for financing a solution. In most cases, the CISO should demonstrate an unambiguous operational efficiency if the intent is to implement new solutions. Furthermore, according to various senior executives, the number of security systems might be restricted. For this reason, some cases will require the CISO to show how a new solution will actually reduce the number of systems in existence and provide the best holistic solution, which will mitigate as much risk as possible. For example, an acquisition of an endpoint detection and response (EDR) and deep packet inspection (DPI) solution, combined with an antivirus module in one agent, can replace a set of systems, such as a current antivirus (AV) software, forensic and remediation agent, anomaly detection tool, incident response management system, control management system, tapping and network analysis tools, and intelligence feeds. In some situations, it can also be used for infrastructure troubleshooting.

• Meet the demand for a formal risk management process. When all efforts have been made and an unsatisfactory decision is inevitable, the CISO should document the formal decision and include a professional and detailed risk assessment. The CISO should not forget that the position serves the organization for better or for worse, although sometimes this service includes facing senior managers with the threat landscape and the information security risk it presents. In this regard, it is the CISO’s duty to pursue due care and due diligence on the given situation, which should include a proper risk management process before any decision is made concerning the purchase of security systems, change management, implementation of new policies, etc.

Conclusion

Although the statement that information security professionals should act as business enablers might be a cliché, it should remind CISOs that they are here first and foremost to serve business needs. Therefore, they must make the best out of their available resources and their position in the organizational layout. One might think this sounds like CISOs should act as yes-men, but that is not the case. Whenever CISOs or any other information security personnel find themselves in a dispute over resources or policies with IT personnel, they should remember one of the most important fundamentals in information security—the risk assessment process. CISOs are expected to hold extensive knowledge in analyzing and presenting the cyberthreat landscape of the organization to its executives, and the proper technological solution or process to mitigate the risk to which the organization may be exposed.

Endnotes


3 A cybersecurity system, in this case, can be an automated vulnerability scanner, upgraded endpoint protection, deep packet inspection, etc.


5 CIO Staff and CSO Staff, “Eight Reasons the CISO Should Report to the CEO and Not the CIO,” CIO UK, 6 January 2017, https://www.cio.co.uk/it-security/eight-reasons-ciso-should-report-ceo-not-cio-3634350/


Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift

Is the chief information officer (CIO) role still relevant for IT security in healthcare? The world of information and data management is changing faster than anyone could have predicted a few years ago, and attention to sensitive data protection is growing, as the new European Union General Data Protection Regulation (GDPR) is clearly proving. The role of the CIO as the custodian of information and data, in healthcare or other contexts, is increasingly becoming paradoxical in many ways.1 One of the crucial pain points of healthcare CIOs is definitely security, albeit IT security is not in any way a neglected item in CIOs’ agendas.2015 was an annus horribilis for data breaches in healthcare, with more healthcare records stolen than at any other time since records started being kept in the United States. According to a 2016 mid-year summary on data breaches,2 the trend is persistent: In June 2016, more than 11 million patient records were exposed in the United States and 2017 followed the same trend regarding the number of reported breaches, although the number of records exposed was lower than previous years.3 Figure 1 shows the status of worldwide data breaches from 2011 to 2017 as explained in the 2018 Italian Association for Cyber Security (Clusit) Annual Report.4 The report collects data about known breaches worldwide from public sources. It is impressive to note the steep increase in healthcare breaches from 2015 to 2016 (up 103 percent), with a further increase from 2016 (73 events) to 2017 (80 events).

An analysis of data breaches shows they can be classified according to six main categories.5

- **Cybercrime hacking**—This is a common scenario, not necessarily involving high-level cyberskills. The easiest way to bypass hospital security is to spear phish workers, inducing them to click on malicious links.
- **Loss or theft of mobile devices and media**—Sensitive data are everywhere, quite often outside the IT-secured infrastructure. Mobile devices are, by nature, subject to theft and loss and, in many cases, the absence of encryption on the devices results in unwanted sensitive data leakage.
- **Insider accident**—A well-intentioned worker performs an action resulting in unauthorized access to sensitive data.
- **Business associate**—A third-party organization working for a hospital experiences a data breach involving clients’ sensitive data.
- **Malicious insider fraud**—This is one of the more dangerous types of data breaches. It is often said that it is difficult to protect an organization from outsider attacks and almost impossible from insiders.
- **Insider snooping**—A worker accesses patient data without any legitimate need to do so.

---

**Figure 1—Worldwide Data Breaches 2011-2017**


---

**Giuliano Pozza**, CGEIT, e-CF Plus (CIO), ITIL v3
Is a biomedical engineer by training and the chief information officer (CIO) of Ospedale San Raffaele, the most important private clinical and research institution in Italy. He is also the president of the Italian Association of Healthcare Information System Professionals. Previously, he was the CIO of Fondazione Don Carlo Gnocchi Onlus, a statewide Italian social care and rehabilitation organization. He also worked for Istituto Clinico Humanitas and in the healthcare practice of consulting firm Accenture.

---

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

Paradox 1: Are There More Things in Shadow IT Than in Official IT?

“There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy.” It seems like “a long time ago in a galaxy far, far away” when IT systems were confined to a well-defined number of applications managed by the IT department. It was a different time and, it seems, a different galaxy. Of course, non-IT departments (e.g., marketing, production, human resources [HR]) sometimes circumvented traditional IT and set up departmental systems. However, it was not so difficult, if needed and desired, to comprise such systems (often called shadow IT, or IT solutions not managed by the IT department) in official IT. For many companies, it was an unspoken strategy to let single departments “experiment” with local applications and then select the best solutions to be included in corporate IT. In a way, if a proper governance model was in place, IT never lost control.

Then the cloud came, with its powerful and fascinating stack of services: Software as a Service, Platform as a Service and Infrastructure as a Service. It represented a bounty of opportunities for users and departments to develop shadow IT solutions with unprecedented possibilities. The traditional IT department, as more often than not happens during a decisive revolution, applied the same governance model as the pre-revolution era, letting users experiment with new technologies and trying to capture the best of breed for corporate IT. Many IT departments are probably still pursuing this strategy. They scout the cloud for the best solutions, they use different cloud solutions themselves and they assume they know what their users are doing and why.

Here is a typical "hyperopia" problem, i.e., a common type of vision error where distant objects may be seen more clearly than objects that are near. An interesting Cisco report states that IT departments estimate their companies are using an average of 51 cloud services. The same report evaluated that in an average company, 730 cloud services are actually being used. Another enlightening report was published recently by Logicalis. The company interviewed 420 CIOs in Europe, North America,

Other sources differ slightly on the classification and the wording, but all agree on these types of data breaches.

The likelihood of a data breach is correlated to the explosion of data. One industry expert estimates that the overall volume growth of data storage requirements in the healthcare sector is doubling every 18 months (another variation of Moore’s Law). The growth encompasses all types of data, from structured data in the electronic medical record (EMR) to unstructured and imaging data. However, imaging and unstructured data, the worst condition from a security standpoint, are the real fuel of this data explosion.

"WITH THE CONTEXT BEING SO CHALLENGING, THE CIO ROLE IS POTENTIALLY CRUCIAL FOR SECURITY IN HEALTHCARE AND FOR COMPLIANCE WITH THE GDPR."
Robotic systems—The use of robotic systems is becoming a standard practice in some specialties. Probably the most famous is the Da Vinci Surgical System by Intuitive Surgical. A report offers a good starting point to grasp the concept of the diffusion of robotics, for example, in urology.¹³ Both are US Food and Drug Administration (FDA)-approved devices, and both can be used in a network to support the “remote presence” of a physician or a surgeon.

Paradox 2: In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a “No Man’s Land” (Call It Shadow IT or Not).

If paradox 1 spans across virtually every market, things become more interesting when the focus moves to healthcare. Besides “official” IT managed applications, there are a number of critical information and automation systems usually passing undetected under the radar of IT departments, such as automation systems of different kinds and medical devices’ data systems (MDDS). These embrace a broad perspective, taking into account both information and automation systems, since from the security point of view, they are both crucial. Automation systems are unevenly spread in hospitals, whereas MDDS are significantly present in every hospital.

Following is a short list of technological systems, which are usually software-controlled and network-connected systems, falling in a sort of “no man’s land” regarding IT governance and security.

Needless to say, these kinds of systems have a vast attack surface and potentially high risk:

• Building automation systems (BAS)—Most modern hospitals include “by design” systems to monitor and control lighting; heating, ventilation and air conditioning (HVAC); energy usage; security; fire; and elevators. In other cases, a complete or partial BAS infrastructure is installed over an existing hospital, including video surveillance data. Since hospitals are, more often than not, composed of many connected locations, the BAS infrastructure frequently controls a considerable number of buildings. A security attack on such a system could have a deep impact not only on hospital security, but on people safety as well.

• Medical devices and MDDS—According to the FDA:

> Medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers with microchip technology and laser surgical devices. In addition, medical devices include in vitro diagnostic products, such as general purpose lab equipment, reagents, and test kits, which may include monoclonal antibody technology.¹⁴

Nevertheless, the category of medical devices also includes highly complex electronic radiation-emitting products and diagnostic equipment. Examples include diagnostic ultrasound products, x-ray machines and medical lasers. Medical devices are broadly used inside and outside hospitals. Medical devices were historically stand-alone stations with no supervisory module. The subset of medical imaging devices normally connects via a picture archiving and communication system (PACS) to
share imaging data, and laboratory systems have a dedicated automation and data management solution called laboratory information systems (LIS). PACS and LIS are well-defined objects subject to specific regulations and usually (but not always) managed by the IT department. Besides LIS and PACS, other medical devices are often equipped with MDDS, as defined previously, and this is a gray zone with respect to IT security. A data breach (or a loss of data integrity) on such systems can have significant consequences.

“SOME IMAGING DEVICES MAY NOT BE EQUIPPED WITH ANTIVIRUS SOFTWARE, AND USUALLY THE OPERATING SYSTEM OF THE WORKSTATION ATTACHED TO A MEDICAL DEVICE IS NOT PATCHED REGULARLY (SOMETIMES IT IS NOT INCLUDED IN THE PATCH MANAGEMENT PROCESS AT ALL).”

Interesting situations are emerging in which building/room automation, MDDS and robotics converge in a complex SCADA system. For example, the Therapy Imaging and Model Management System (TIMMS) is a complex system to integrate and manage heterogeneous medical devices, clinical information systems and components of computer-assisted surgery in the operating theater.15

This example makes evident the convergence of IT with operating theater automation and medical device management. The consequence of this kind of technology evolution and convergence is that the “no man’s land” is getting wider and wider, sometimes exceeding the land under the governance of IT or the clinical engineering department. It is not exactly shadow IT, since these systems are, in a way, official technologies, but from the security perspective, they are unmanaged systems in many hospitals, exactly as shadow IT is.

Going further, the medical devices managed by clinical engineering are a potential security threat as well. For example, some imaging devices may not be equipped with antivirus software, and usually the operating system of the workstation attached to a medical device is not patched regularly (sometimes it is not included in the patch management process at all). Moreover, bring your own device (BYOD) policies, applied in many hospitals without proper governance and risk limitation practices, and issues with implantable medical devices16 pose new and unprecedented threats to security and safety in the hospitals. The recent field action by the FDA on Abbot Laboratories, requiring a firmware update to address cybersecurity vulnerabilities in implantable cardiac pacemakers, is a striking example of the level of security issues that exist in healthcare today.17

Again, the trend is more cogent in healthcare (where a security problem on a SCADA system controlling an operating theater could have frightening consequences), but it is analogous to what is happening with SCADA systems in other industries as well. A 2012 Accenture report provides an interesting overview of the phenomenon.18

Paradox 3: CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend.

The traditional approach to IT security is focused on strengthening the security of IT systems. If this statement seems purely tautological (and it is), it is important to consider the implications. The previous paradoxes demonstrate that technology systems (IT or automation) outside IT department borders are growing and sometimes exceeding traditional IT systems. Moreover, in healthcare, the most vulnerable (and sometimes dangerous) systems are probably the ones outside the IT perimeter. Using a metaphor, IT professionals are spending a good
The first U-turn consists of redefining the vision of IT security, where a key point is to select the right analogy. As explained previously, the goal cannot be the defense of a citadel, but rather the protection of an open city with a wide attack surface. It is necessary to manage at a different security level and it is possible to even plan to secure or seal up portions of the city (critical buildings or infrastructures) when it is under attack, but walling the city is not an option nowadays. This is not far from the approach used to protect critical infrastructure. One interesting example of this approach applied to healthcare infrastructure is the Terrorist attacks on Hospitals: Risk and Assessment, Tools & Systems (THREATS) project, part of the European Union’s European Programme for Critical Infrastructure Protection (EPCIP).

The second U-turn is to move from a siloed approach (equivalent to fortifying a portion of a wall) to an integrated and holistic approach to security. All the information and automation technologies in the hospital must be addressed, regardless of who is responsible for what. A strategy purely focused on IT department borders is nonsense. Security must go beyond outdated borders and embrace traditional IT, cloud, clinical engineering, building automation, and all the subcategories of shadow IT that handle relevant and/or sensitive data or operations.

Technology

Technology can be an enabler of an integrated and holistic approach to security. This can be addressed in two directions:

1. In technology assessment and acquisition, it is important to ensure that security is one of the basic requirements, included by design in the technology under evaluation. This was straightforward in the past, but it is quite a challenge nowadays due to the manifold variety of technologies involved (traditional IT, user-acquired cloud services, medical devices, robotics and automation). The task of assessing new technologies cannot be accomplished by one department alone without coordination with IT and other technical departments. A clear example of the importance of a cross-border approach is the selection of an endpoint security tool. Traditional antivirus software is a (partial) answer for end-user workstations, but in many cases, diagnostic equipment workstation producers will not allow IT to install antivirus
software. Actually, the solution is just around the corner: IT should select end-point protection software based on the integrity monitoring principle. The software will compute a hash code of the system files and alert the users (or the IT/clinical engineering departments) if the system files change compared to a certified baseline. This approach is a common technique used on SCADA systems, but it is often overlooked in healthcare because, since integrity monitoring is hard to apply to traditional clients, it is usually not included in the requirements the IT department considers essential for an antivirus solution.

**THE POINT IS NOT TO HAVE THE BEST ANTIVIRUS, THE MOST EFFECTIVE FIREWALL OR THE TIGHTEST DATA LOSS PREVENTION (DLP) SOFTWARE, BUT TO BUILD THE BEST INTEGRATED AND MULTIDOMAIN-ENABLED SECURITY ARCHITECTURE.**

2. In selecting the tools and services (e.g., security operation centers [SOCs]) to support security, the IT department should incorporate an architectural vision more than a mere evaluation of a single product in a traditional best-of-breed approach. The point is not to have the best antivirus, the most effective firewall or the tightest data loss prevention (DLP) software, but to build the best integrated and multidomain-enabled (e.g., IT, clinical engineering and automation) security architecture.

**Processes**

Processes and methodologies must be updated as well. Presently, the IT department has a set of core methodologies for governance and security (e.g., IT Infrastructure Library [ITIL], COBIT® 5, International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] ISO/IEC 27001), while clinical engineering is working on a different set of methodologies (e.g., a health technology assessment [HTA]). This was fine a few years ago, when diagnostic equipment was purely machines. Now, the data-capture devices (such as medical devices with their MDDS) and automation technologies are mostly software-defined and software-controlled: A new methodology set and new processes are needed to guide the way new technologies are assessed, implemented and run.

**People**

People and organizational structures are among the crucial topics in every human endeavor. As this article has described, many healthcare organizations do not take into account the underlying technology convergence. The three typical technology departments in a hospital (i.e., facility, clinical engineering and IT) were born when buildings were walls and bricks, medical devices were dumb machines, and IT managed a well-defined set of applications and data. Now, buildings are Internet of Things (IoT) ecosystems generating critical and continuous streams of data, software-controlled robotic systems (ranging from logistic management to surgery) are both data generators and critical infrastructure components, and IT is scattered in hundreds of internal and external services. Many organizations are reacting with the establishment of a unified technology department. This is not a new trend: A 2006 article proposed convergence between IT and clinical engineering.\(^2\) If a convergence between IT and clinical engineering is not possible, at least a chief information security officer (CISO) should be appointed, reporting directly to the chief executive officer (CEO), not to the CIO.

Furthermore, a cross-section of different skills and competencies should be the objective of every technology organization that aims to build a common culture and awareness about security themes. The 2018 Emergency Care Research Institute Report highlighted cyberattack as the top hazard for medical devices.\(^2\) Therefore, IT professionals should be aware of the specifics of medical devices, and clinical engineers should be trained in the essentials of IT security.

The methodology frameworks (this time, for people management) should evolve. For example, the European Community is standardizing IT professional profiles around the so-called
Putting the Pieces Together

Setting aside for a moment the big issues with methodology and frameworks, there is a tangible path for hospitals and healthcare IT organizations that wish to address security and governance in a way that is aligned with the occurring technological convergence and with the accountability principle of the GDPR.

Taking inspiration from the Capability Maturity Model, it is possible to propose a pathway in five stages (Figure 2).

The stages can be defined as follows:

- **Stage 1 (Initial)** — “Local,” not structured, security management exists.
- **Stage 2 (Managed)** — Structured security management for ICT is in place. There is general awareness about security in other technical areas (using the ICT department as the internal expert on call).
- **Stage 3 (Defined)** — Coordination efforts and policies on security are in place among different technology areas (e.g., ICT, facility, clinical engineering), but no dedicated cross-border organization for security exists.
- **Stage 4 (Quantitatively Managed)** — A cross-border role on security (e.g., the CISO reporting to the CEO) oversees security strategy and policies with a 360-degree approach. At the departmental level, security is well managed, with key performance indicators (KPIs) and monitoring processes.
- **Stage 5 (Optimizing)** — This is a converged security strategy and organization. The technology departments in the hospital are under a unified responsibility. Security and governance are managed with a holistic approach.

It is likely that any hospital, with due time and resources, could reach the Defined stage; going farther is more complicated. Reaching level 4 is more difficult (“hic sunt leones”), since it requires a strong commitment and a cross-departmental approach.

If stage 5 seems too bold, it is worth considering this insight when discussing a broader context during a Cisco workshop:

IoT is made up of a Communications Internet, an Energy Internet, and a Logistics Internet that work together in a single operating system, continuously finding ways to increase thermodynamic efficiencies and productivity in the marshaling of resources, the production and distribution of goods and services, and the recycling of waste. [...] Together, these three operating systems comprise the physiology of the new economic organism. The three interoperable Internets of the IoT require a transformation.
in the functions of every enterprise. [...] I expressed my doubts about the viability of chief information officers (CIO) in an evolving IoT economy and suggested that in the future, IT, energy services, and logistics would be integrated into a single function under the supervision of a chief productivity officer (CPO). The CPO would combine IT expertise, energy expertise, and logistics expertise with the aim of using the IoT to optimize the thermodynamic efficiencies and productivity of the company’s operations.27

This new holistic approach to security, governance and organization is the real game-changer. The cultural convergence of different professions, more than a pure organizational or technical convergence, is what will enable healthcare CIOs (and maybe other CIOs as well) to survive what can be defined as a perfect storm, or, from a more optimistic point of view, a perfect opportunity.

Endnotes

1 Heller, M.; The C.I.O. Paradox: Battling the Contradictions of IT Leadership, Routledge, USA, 2012
4 Clusit, Rapporto Clusit 2018 sulla sicurezza ICT in Italia, CLUSIT, Italy, 2018
6 A generally accepted computing rule stating that computer processing speed doubles every two years. Moore’s Law, www.mooreslaw.org/
8 Shakespeare, W.; Hamlet, 1603
9 As seen in the opening sequence of every numbered film of the Star Wars series
12 Ibid.
14 US Food and Drug Administration, “Is the Product a Medical Device?” USA, www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm
17 US Food and Drug Administration, “Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott’s (Formerly St. Jude Medical’s) Implantable Cardiac Pacemakers: FDA Safety Communication,” USA, 29 August 2017, https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm
23 ECRI Institute, Top 10 Health Technology Hazards, ECRI, 2018
25 CMMI Institute, http://cmmiinstitute.com/
26 “Here are the lions,” meaning to say that this is the crucial point.
27 Rifkin, J.; The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism, St. Martin’s Griffin, USA, 2015
The exposure of data for up to 14 million of Verizon’s customers in July 2017 was an enormous embarrassment, particularly for an organization that presents itself as a premium cybersecurity consultancy. After all, Verizon produces its Data Breach Investigations Report (DBIR) annually, which documents the largest cyberthreats its customers could face in the upcoming year and how to avoid them. The irony is that Verizon itself has now become a data point for its future reports.

As has happened in other breaches, an external vendor was responsible for the incorrect settings that allowed open access to Verizon user information. This incident reinforces the concern regarding how security professionals can stay on top of all the data and all the different configurations extant in departments across the enterprise. The good news is that, in recent years, many IT organizations have initiated master data management (MDM) projects to help rectify this situation.

Having standard configurations that are documented and staff that is trained to follow these standards helps. But it is well known that one of the biggest risk factors is people—and people make mistakes. Whether intentional or not, mistakes introduce the opportunity for breaches. One of those mistakes can occur when an organization's cybersecurity team is not involved as a stakeholder in IT projects such as MDM.

What Is MDM?

MDM is an effort to rationalize disparate and overlapping databases to ensure the accuracy, integrity and consistency of corporate data. Multiple databases with multiple versions of data that might not be consistent across an organization's database landscape can be caused by silos within the organization, mergers and acquisitions, and other issues.

The most common example of why this is a problem is when a customer’s information is not accurate across all databases. This can cause damaging miscommunications with customers that can, ultimately, harm the organization’s reputation.

There are two methods for collating data in an MDM environment: consolidated and federated. In a consolidated system, the data are collated and distributed from a centralized source. In a federated system, there is a virtual view of the data, which are collated and distributed from multiple sources.

Why MDM Is a Cybersecurity Concern

In a time when MDM and business intelligence (BI) are common terms in the business world, organizations are still trying to figure out how to keep data fresh across multiple systems and, of greater challenge, how to report on the data. The larger concern for any security professional is the fact that data hold significant corporate risk.

With personally identifiable information (PII), the US Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), the US Sarbanes-Oxley Act (SOX), and the EU General Data Protection Regulation (GDPR), to mention just a few overarching laws and regulations that govern how to protect data, the difficulty comes with knowing where all the data are.
going and how they are being used. Are they stored in a distributed fashion, traversing multiple networks and residing in multiple data centers? Does anyone in the organization really know? There is seldom a data diagram that maps out where all information is stored. Even the MDM team struggles to keep track of every new application and reporting tool that pulls data to yet another place.

These unknowns bring MDM under the scope of risk management. While many will turn to a framework such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27000 series or US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and take a compliance approach, there are many examples of compliance failing to protect sensitive information.

Yet another business risk lies in the shadows, where there is no real oversight. Most cybersecurity professionals never consider the quality of information to be a security risk. But, if incorrect information regarding a serious problem is released, the reputation risk can affect the organization’s revenue. Once that happens, recovery is difficult and sometimes almost impossible. Given the scope of this type of risk, one of the considerations should be at what point the operational risk team should be involved.

THE CYBERSECURITY TEAM CLEARLY SHOULD BE INVOLVED AS A STAKEHOLDER AT THE BEGINNING OF ANY MDM INITIATIVE TO HELP DEFINE AND APPLY THE RELEVANT CYBERSECURITY STANDARDS AND POLICIES.

MDM Governance
In some cybersecurity groups, the term “governance” is used interchangeably with “compliance.” In this article, the term “governance” is defined in congruence with corporate governance with regard to decision rights: who owns what decisions at what level regarding MDM. Obviously, this needs to be defined up front.

The details of an organization’s governance design for MDM will be decided within the current corporate/IT/cybersecurity governance framework in place within the organization. The following MDM governance delineation recommendations can serve as a starting point for discussion:

• The business owns the decisions regarding the data and applications, but not the tools or processes surrounding the data.
• IT owns the decisions on physical data storage, the platforms/locations for the applications that use the data, and the tools and processes surrounding the data.
• The cybersecurity team owns decisions regarding securing MDM and the data.

MDM in the Cybersecurity Domain
So what should the cybersecurity team be doing to minimize and mitigate the risk inherent with MDM? Properly securing MDM is similar to securing other applications, processes and data. There are five areas that should be given consideration:

1. MDM governance
2. The initial MDM project
3. The standards and policies surrounding MDM
4. Securing MDM tools
5. Securing MDM processes

The Initial MDM Project
The cybersecurity team clearly should be involved as a stakeholder at the beginning of any MDM initiative to help define and apply the relevant cybersecurity standards and policies.

The cybersecurity team’s relationship with the enterprise’s IT organization and users should be good enough that the team is informed of data-involving projects during the planning/initial stages. That being stated, the team must be constantly watchful for MDM projects (or any data-involving projects, for that matter) as the business and IT organizations may not always understand the need for the team’s requisite involvement.

At a minimum, cybersecurity should be a participant in the architectural committee that reviews every project during the planning and kickoff phases.
Securing the firm’s MDM tools is no different from applying cybersecurity standards and processes to other IT applications. It is important to be absolutely certain that the tools’ security settings are optioned correctly and the organization’s identity and access management (IAM) policies and procedures for accessing the tools are firmly in place and regularly reviewed for compliance. In addition, care should be taken to ensure that the cybersecurity standards for security patching are followed.

Securing MDM Processes
Depending on the organization and how the cybersecurity team is involved in IT projects and implementations, MDM can be reviewed as a part of the software development life cycle (SDLC) process, another consideration for the architectural review board or an item for the change control process. The key is to have the requisite opportunities to assess the data, their sensitivity and how they are being protected. One review is not sufficient, as many times over the life of an application the data will be manipulated, which can change the data’s security requirements.

Recent data breaches and data exposure incidents indicate that third parties represent one of the greatest vulnerabilities today. With this in mind, it is important that the cybersecurity team tackles...
the role of reviewing contracts with third parties and ensuring ongoing compliance with them. This is necessary to assure strong data protection requirements, define acceptable protection methodologies, define responsibility in the event of a data breach, mandate cyberinsurance levels and outline the appropriate media response if there is a breach.

**Getting Started**

If the organization's cybersecurity team is not already involved with the MDM efforts, it either should be or soon will be, as the enterprise and IT organizations take advantage of MDM's benefits. Hopefully, the roles and responsibilities for each team are well defined, which will make the cybersecurity team's involvement in these new efforts more productive.

The conversation with the MDM team can begin with the fact that data are powerful assets that warrant five-star security and the cybersecurity team wants to help the MDM team protect its data. Demonstrating respect for the value of both the data and the MDM team will help build a relationship based on common interests. It is critical to avoid being heavy-handed, as this will quickly sour the relationship between the teams.

As rapport is established, the project's documentation can be requested. After in-depth study, it is advisable to start with the basics of encrypting the MDM data both while at rest and during transit, with a focus on sensitive, valuable information. After encryption is addressed, it is possible to begin applying the rest of the cybersecurity organization's standards and policies to the new project, including IAM, patch management and data retention. This will allow the MDM team to continue to own data responsibility while incorporating a cybersecurity view.

Any new technologies or processes that will be required by the project must be analyzed and, if required, new cybersecurity standards and/or policies developed to cover them. Also, it is important to identify any tools that will be used so the cybersecurity team can ensure they are secured. On an ongoing basis, the strength of the security of any access tools that may be used by the firm's data analysts should be evaluated.

To properly secure the MDM data in the future, detailed data maps must be developed and maintained over the life cycle of the data. After the initial MDM implementation, the security of its data and procedures must be included in the organization's standard review processes.

Ultimately, the most important thing is that there should be trust, mutual respect and strong working relationships among IT, the business organization and the cybersecurity team. Not having those relationships in place can expose the organization to cyberrisk.

**Endnotes**


Secure Elections in a Smart World

When people hear the term “cyberwarfare,” there are a few things that come to mind. The things people visualize tend to be the high-impact, “scare the pants off you” scenarios such as those one might read about in a thriller novel or see on television. For example, a rival nation disrupts a country’s power grid, purposefully bringing about industrial accidents to cause harm, interrupting communications, interfering with public services (e.g., opening dams to cause floods) and so forth.

These are, of course, very real things that could happen. In fact, they have occurred in actual practice. Stuxnet, for example, is widely believed to be a cyberweapon created for the specific purpose of disrupting the Iranian nuclear program. Another example is the (Not)Petya outbreak that caused so much disruption in the Ukraine. It is widely theorized that this attack was a cyberwarfare campaign designed around that specific purpose. Since nations are notoriously tight-lipped about their offensive cybersecurity capabilities, it is unlikely that there will ever be irrefutable proof that either of those examples was, in fact, cyberwarfare—but Occam’s Razor tends to lead to the conclusion that they probably were.

Despite the images that the term “cyberwarfare” tends to invoke, however, there are techniques that, while equally disruptive over the long term as the examples above, operate with more subtlety and are much less directly visible to those they impact. For example, consider the possibility of systematic and targeted attacks against the democratic process—in particular, subverting or influencing a specific election outcome.

Now, in some places, this is a loaded topic. For example, there are discussions currently underway in the United States political realm about whether or not this was a factor in the most recent US presidential election. Despite that, though, most everyone can agree that having a secure, accurate and reliable result from an election is important to any democracy. And, regardless of where one stands on any given example of election tampering, most everyone can agree that the stakes are high enough to warrant candid discussion about the possibility as elections become more automated and technology is more frequently used to directly support them.

**State of the Community: Election Security**

It was with this in mind that ISACA, as part of a broader investigation about secure government (in particular, smart cities), surveyed its members related to their confidence in governments to ensure accuracy, reliability and security in the election process. Respondents were varied across disciplines, including those from the audit, security, risk, governance and compliance fields. The one

---

Ed Moyle

Is a founding partner of the analyst firm Security Curve. Prior that, Moyle was director of thought leadership and research at ISACA. In his nearly 20 years in information security, he has held numerous positions including senior strategist with Savvis, senior manager with CTG’s global security practice, vice president and information security officer for Merrill Lynch Investment Managers. Moyle is coauthor of Cryptographic Libraries for Developers and a frequent contributor to the information security industry as an author, public speaker and analyst.

---

Do you have something to say about this article?

Visit the Journal pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

thing they have in common: They all share a commitment to “trust in information and information systems.” Who better to ask?

THE OVERWHELMING MAJORITY OF RESPONDENTS LACK CONFIDENCE IN THE ABILITY OF GOVERNMENT TO ENSURE THE SECURITY OF THE ELECTION PROCESS.

The specific questions asked were in the abstract, without attention or focus on any specific region, individual election or set of elections. Two questions were asked, related to:

• Whether practitioners had confidence in the ability of governments to ensure secure, reliable and accurate outcomes from the election process
• The level of government that should have accountability for ensuring the security, accuracy and reliability of the election process

Approximately 2,000 people were surveyed (1,954, to be exact) and what they said was striking. First, the overwhelming majority of respondents lack confidence in the ability of government to ensure the security of the election process (figure 1). Eighty-four percent were at least somewhat concerned about the ability of the public sector (i.e., government) to conduct secure, reliable and accurate elections.

Respondents were also asked about who in government should be responsible for ensuring the security of the election process. Respondents were asked to select the areas of government where responsibility lay for securing the election process; multiple selections were allowed (as one can imagine multiple levels of government having a role to play here) (figure 2). Results here were more split, with most (71 percent) believing that the national government should have responsibility. State (51 percent), county (40 percent), city (41 percent), and regional (23 percent) government were seen as having a role, but by a much smaller factor (20 percentage points). In addition, 14 percent of respondents also saw nongovernment institutions (e.g., the media or private enterprise) having a responsibility as well.

Implications

Given the impact that elections have for any democratic nation, the importance that members place on ensuring that outcomes are fair and reliable should, perhaps, not be surprising. Likewise, given
that election outcomes are of national significance, readers should, perhaps, also not be surprised that most view the national government as being the most accountable entity to ensure it. That said, the fact that these results are what they are has a few implications for the industry and, perhaps, for society at large.

First and foremost, this should serve as both an area of opportunity and potential warning—both for government and the industry. Specifically, it is a fact that elections are becoming more automated, with increasing levels of support from technology. It is important that systems are built that can bolster confidence in the outcomes of the elections they support. This is why it is both an area of opportunity, but also concern. On one hand, automated systems appropriately designed and hardened can help underpin confidence in a secure and trusted election process while increasing voter convenience at the same time. By contrast, when those systems leave something to be desired from a security point of view, the opposite can be the case.

Additionally, for jurisdictions where the national government has a minimal role in the security of the election process—for example, in the United States where the state and local government have the most direct oversight—the fact that citizens see the national government as being the entity that should play the most active role is an issue and food for thought for policy makers.

"This should serve as both an area of opportunity and potential warning—both for government and the industry."

Endnotes


Figure 2—Survey Responses to Question 2

Who should have responsibility for ensuring that elections are secure, accurate and reliable? Select all that apply.
IT professionals and enterprise board members live in two very different worlds. Boards worry about strategic concerns such as revenue, share price and brand reputation, whereas IT staff are paid to deal with operational challenges such as those stemming from big data, cyberthreat actors and cloud usage. Bridging the gap between these strategic priorities and day-to-day concerns to initiate an organization’s technological transformation can seem insurmountable.

In any enterprise transformational program, people, processes and technology are key ingredients to long-term success. Information governance (IG), which is an operational approach to managing the valuation, creation, storage, use, archival and deletion of data within an organization, is no exception. Proactive IG requires collaboration among legal, compliance, security and IT teams to take an incremental, measurable approach to deal with today’s enterprise data challenges. Such cross-functional collaboration almost invariably requires an executive or board-level mandate. Often, however, absent fines, litigation and/or regulatory scrutiny, IG is not sponsored at the board or executive level. What can stakeholders in an IG program do to obtain the level of executive or board sponsorship necessary to ensure success?

In one recent client engagement, consultants helped legal counsel get a seat at the table and engage top enterprise leadership in establishing IG to mitigate risk around impending litigation. Conversely, consultants have also worked to help clients restart projects that have stalled due to competing demands within a cross-department project team.

Traversing the Gap

Failure to handle data properly often results in damaging data breaches, which have been estimated by the Ponemon Institute to cost US $3.62 million on average.\(^1\) Beyond this and legal/compliance violations, breaches break trust and cause reputational damage. The key to obtaining C-level and/or board involvement in an IG initiative is to position its benefits as specifically addressing risk and brand reputation, rather than as operational improvements.

An organization’s risk framework to prioritize its highest risk, such as regulatory/sanctions or reputational damage, can help an IG team evaluate which risk categories an IG program will impact, and make a cost-effective business case for it. Some of today’s most pressing data risk scenarios include:

- **Big data**—Organizations have deployed numerous software systems—legacy and new—with data stored in many different places and ways. The Leading Edge Forum Data rEvolution study predicts that by 2020, 100,000 organizations will store one or more petabytes of data.\(^2\) Organizations are managing rapidly evolving and heterogeneous data ecosystems spanning personal computers, mobile devices, social media...
and a myriad of cloud-based collaboration tools, often with little insight into how information is created or managed. The proliferation of this dark data creates a level of disorganized complexity, causing confusion, security risk and increased costs for finding data when litigation, regulatory or investigatory mandates arise.

• **GDPR and privacy**—The European Union General Data Protection Regulation (GDPR) will impact many facets of business for multinational corporations. The GDPR requires organizations based in the European Union and those that retain personal data of EU citizens—including any information related to an individual, such as physical address, email address, Internet Protocol (IP) addresses, age, gender, global positioning system (GPS) location, health information, search queries and items purchased—to meet stringent data protection requirements. Many organizations that freely harvest and commercialize this information today will be required to bear the cost and risk of these requirements. Failure to comply can lead to fines of up to 4 percent of a company’s global annual revenue or EU €20 million. Because the regulation is so expansive and new, just knowing where to begin is challenging.

Included in the GDPR is an erasure, or right-to-be-forgotten provision, that gives EU citizens the option to require their PII to be erased from an organization’s databases and other systems and made inaccessible to others seeking that information. Legal and IT teams must understand possible interpretations of this and other data-subject rights in the GDPR and be equipped to communicate the implications of noncompliance to the board.

• **Cybersecurity**—Data security is now an enterprisewide endeavor and a major concern for boards and top executives. Globally, there are dozens of laws that regulate how corporations manage cybersecurity and what they must do in the event of a data breach. Cybersecurity events seen over the past year demonstrate how extensive the damage of a global attack can be. Attacks and ransomware will continue to hit private and government networks around the globe, and threat actors will continue their increasingly sophisticated cyberaggression. As cybersecurity threats and regulations evolve, it is important for organizations to manage cyberrisk holistically, mapping out programs for addressing the unique challenges in each region where the organization does business. An IG program set up to protect valuable business information and the timely disposal of noncritical information contributes to the strong cybersecurity posture mandated by today’s enterprise boards and executive leadership.

**“IMPLEMENTATION OF CLOUD SERVICES INTRODUCES A VARIETY OF IG-RELATED RISK FACTORS RELATED TO EMAIL ARCHIVING, DATA PRESERVATION, CROSS-BORDER REGULATIONS, DATA SECURITY AND E-DISCOVERY PROCESSES.”**

• **Legal hold, e-discovery and compliance**—Legal hold is another area where poor execution can lead to significant financial and legal risk, but which can be addressed by proactive IG. This process requires close monitoring to ensure its defensibility and to guard against possible spoliation charges in litigation, which can come with steep penalties. It can be difficult for organizations to scope the correct individuals who need to be under legal hold and limit preservation to only those individuals. Legal teams are critical
With cross-functional support, stakeholders can demonstrate how specific IG initiatives can directly reduce reputational and other key risk and gain support from the board. Projects that can help ensure safe and responsible handling of sensitive data, strong compliance and business process efficiency include:

- **Eliminating legacy data and adjusting policy**—Remediate legacy storage by refreshing backups, disposing of redundant backup tapes and establishing an enforceable archiving policy. To remediate legacy back-up tapes, legal and compliance teams must collaborate with IT to take inventory of and address any regulatory and legal-hold obligations on the data. This process can also be a forcing function to standardize legal-hold policies, potentially saving significant long-term storage and e-discovery costs.

- **Digital transformation**—Many organizations are undertaking digital transformation efforts involving migrating data to the cloud. Microsoft Office 365 alone has more than one million monthly commercial users, and Microsoft indicates adoption is growing rapidly. Implementation of cloud services introduces a variety of IG-related risk factors related to email archiving, data preservation, cross-border regulations, data security and e-discovery processes. The movement of critical enterprise data to the cloud raises security and data protection concerns, and studies have shown the incidence of advanced email threats rising for organizations of all sizes. For all these reasons, cloud migration and other digital transformation efforts aimed at business process optimization and improving cost efficiency should be viewed as critical initiatives.

- **Bringing unstructured data under control**—Most organizations store unstructured data that include confidential data or PII that may be subject to privacy laws. Taking the time to scan file shares for sensitive data, identify critical information, and get it under lock and key can help mitigate the risk of loss of intellectual property and trade secrets, and the operational and reputation risk involved with managing a data breach.

- **Modernizing message archiving**—Email archives are one of the most undermaintained systems within an organization, and most archives are built on aged technology that desperately needs to be

---

**One Step at a Time**

IG is often thought about in the context of IT efficiency, data security and regulatory compliance. While it is true that these are the most critical drivers for executing data and information governance programs, the equally important factor of brand reputation deeply resonates with an organization’s board and C-suite. Projects may be driven by a variety of internal sponsors, all bringing varying needs and goals to the table. The chief financial officer (CFO) or finance department may be looking to reduce year-over-year spending by remediating data and increasing storage efficiency. The IT department cares most about mitigating the costs of big data and ensuring that the organization does not suffer from network overload. The legal team is focused on e-discovery, ensuring legal-hold compliance and fulfillment of regulatory requirements. Understanding and leveraging these various drivers can help gain executive sponsorship for the project and make it easier to bring a group of stakeholders together to tackle the implementation.
updated or evaluated for defensible disposition. New archiving technology can provide built-in IG controls and a much better experience for running searches and extracting data for e-discovery or other reasons, as well as for end-user management of email. Features include preset retention policies and the ability to identify sensitive information that is being sent outside the organization so it can be stopped before it leaves the network. An archive modernization initiative provides a good opportunity to show value with IG.

- **Using cloud migration as an opportunity**—Migration to cloud systems provides an opportunity for an organization to take stock of its email and data management practices and potentially update policies and remediate data for greater efficiency and security. Cloud solutions do introduce new IG concerns, including expanded individual storage and retention challenges, but there is also better ability to search and manage the data and significantly reduce storage costs.

- **Moving beyond first-generation e-discovery**—With the broad awareness most organizations and law firms have today around e-discovery, a surprising number of them are still using first-generation tools for search and retrieval. There are a handful of organizations on the forefront of emerging technology, but most still use basic bulk collection from email archives as their primary process for e-discovery. Further, most first-generation tools have trouble with e-discovery from other unstructured data sources such as SharePoint and cloud-based repositories. Collaborative platforms often contain information critical to a case, and the scope of e-discovery has gone well beyond email and traditional electronically stored information (ESI), frequently calling for desktop, file share, and other structured and unstructured data sources. Updating e-discovery processes and technology can enable the legal team to deal with matters that are on their desks today and provide tools to build toward stronger IG.

- **Leveraging analytics/machine learning**—Advanced technology has emerged that can accelerate IG remediation and support in investigations and litigation. Legal and IT teams are just scratching the surface for advanced analytics and machine learning tools that can be applied to advance IG initiatives. These technologies can be useful in taking large amounts of data and classifying them in an efficient way, reducing manual effort and cost.

**Measuring Success**

For a long time, boards have overlooked the inherent risk living within the organization's data. The combination of new privacy laws and the increasingly aggressive nature of cyberthreat actors is changing all that. Top enterprise leadership must start paying attention to these issues to maintain baseline security and compliance. Proactive IG can be an important component to effectively address these challenges and provide other tangible and sustainable benefits.

There is a significant reduction in cost and an increase in efficiency of e-discovery processes when an organization’s data have been properly organized and remediated as part of an IG program. With disorganized, unmanaged enterprise data environments, e-discovery teams have difficulty viewing and managing data across dozens of different file servers, Skype, email, Dropbox, and other data sources. Remediated data environments also make it easier to search and identify PII and other sensitive data such as credit card information and government identification numbers, helping to meet privacy obligations and take necessary remediation steps such as securing, encrypting, and/or deleting sensitive data. IG enables teams to more efficiently conduct a detailed analysis of security weaknesses and gaps, and proactively monitor locations where critical data are located and loss is likely to occur.
monitor locations where critical data are located and loss is likely to occur. This makes it possible to put protections in place, as well as reconcile remediation with steps to preserve data required for compliance or legal-hold purposes.

While data issues can be overwhelming, teams must remember that they do not need (nor should they try) to boil the ocean. Instead, data remediation projects can be prioritized by those that address the highest-risk areas or provide a quick-win to give momentum. One way to help prioritize might be to break down IG goals into categories:

- Protecting the sensitive information of customers and employees
- Securing sensitive company intellectual property
- Arming against cybersecurity threats
- Developing protocols and systems to ensure secure access to the network by partners and approved third parties

These or similar subcategories within a broader IG program can help take a large challenge and channel it into initiatives that are more focused, easier to accomplish and supported by the board.

Endnotes
Intellectual Property Protection for High Tech’s Crown Jewels

Theft of intellectual property (IP) is an emerging threat and a topic of boardroom conversation for organizations across the United States, particularly for those in the high-tech industry. One need look no further than the IP Commission Report, updated in February 2017, to see the scale of the risk this issue presents. This report estimates the cost of trade secret theft to be 1 to 3 percent of the US Gross Domestic Product (GDP), which translates to between a sobering US $180 billion to $540 billion. While the government is driving initiatives to curb these losses, organizations should not wait around for legislation that may be difficult to implement or fail to address the source of the risk.

IP theft can prove disastrous. With the possibility of IP thieves invading from both the inside and outside, organizations must address the risk by using a proactive and holistic approach that encompasses people, processes and technology. This requires a comprehensive understanding of the inherent risk associated with IP and, in turn, the implementation of effective management and technical controls.

**The High Cost of IP Theft**

Cases of IP theft and leakage can be devastatingly costly for enterprises. Thieves can leak IP directly to consumers, as happened with some of the HBO content stolen in 2017; or to an organization’s competitors. Either way (and sometimes both scenarios unfurl), thieves can lay waste to existing business strategies and expected revenue sources and leave a path of unforeseen costs as breaches are investigated, diagnosed and remedied.

If a malicious hacker steals IP, the hacker can create an eye-popping bill for the victim, costing an organization extensive time and money to repair any corrupted material and institute precautionary measures to prevent similar incidents in the future. Sony Pictures made headlines in 2014 when employees were greeted with images of a red skeleton on their workstations, alerting them that the studio had been hacked by the “Guardians of Peace.” The studio suffered enormous monetary losses due to the theft of IP assets (including scripts and movies) as well as reputational damage due to the leaking of embarrassing emails. The IT expenses alone cost the company an estimated US $35 million.

The cost for Sony Pictures was substantial, but the company was able to move past the incident and continue its normal operations after making the appropriate responses to protect its remaining IP. However, other organizations that fall victim to IP theft are not always as lucky; for some, the damage runs far deeper.

---

**Ray Cheung, CISA, CITP, CPA**

Is a managing director and leads the high-tech group in risk consulting at Crowe Horwath LLP, one of the largest accounting, consulting and technology firms in the United States. He has more than 25 years of experience in public accounting and private industry, solving business problems by identifying control inefficiencies through implementing technology and control process improvements. Cheung has significant experience providing independent board and senior management-level consulting services in the high-tech sector and across other industries. Previously, Cheung was a managing director in risk advisory services for a national accounting firm and a Big Four firm. He was also the chief information officer for a start-up and vice president of the technology management group at Visa International. Cheung can be reached at ray.cheung@crowehorwath.com.

**Mike Porter, CISSP**

Is a manager in the cybersecurity solutions group of risk consulting at Crowe Horwath LLP. His experience includes system design and implementation projects for a variety of technologies including end-point security, data loss prevention, network access controls, and identity and access management. Porter can be reached at mike.porter@crowehorwath.com.

---
organization might see its public image tarnished, and customers could become reluctant to do business with it for fear that their data will be targeted in the future.

**Risk Factors**

High-tech companies might be particularly vulnerable to IP theft due to several factors.

**International Relationships**

Controlling IP becomes more important, and more complicated, when an organization has international relationships, which is common for tech companies (e.g., a tech company that uses foreign component manufacturers). Global collaboration and coordination can, of course, offer several advantages for product manufacturing and development of IP, but they also can increase the inherent risk of managing the related data. If nothing else, these relationships create an added layer of complexity when addressing legal considerations for patent, trademark and copyright protection. The need to translate IP into another language can also obfuscate the flow of such data.

International relationships can bring the risk of bribery, too. Bribery risk varies greatly from country to country. While the mere existence of bribery risk should not exclude potential collaborators from consideration, it highlights the need for an organization to consider the cultural, economic and political climates of all of its business partners.

**Quantity of IP**

When it comes to IP, an organization can have both a standard and inverse risk relationship with its quantity of IP data. On the one hand, the risk of IP theft follows a standard model, climbing as the quantity of IP increases. On the other hand, though, a limited amount of IP can represent disproportional risk if that IP is essential to the core business activity. The exposure of such IP data could be catastrophic for organizations that rely on a single service, technology or algorithm.

**Format of IP**

The format of IP can greatly affect the ease of management and commensurate controls that an organization can deploy to protect it. For some
companies, IP comes in defined formats and resides in well-controlled repositories: for example, a software development company whose source code is controlled through an enterprise version-control system.

But the format of IP can prove more difficult to understand, define and control in other organizations. When IP takes the form of business processes, technical schematics (in a variety of formats) or creative content, it can be less obvious where controls should be inserted.

Most large organizations find themselves in both boats. Some of their IP is well defined, with a clear inventory and understood business processes, while other IP is hard to define, discover and, ultimately, control.

**Management Controls**

An organization’s management controls are its front line of defense against IP theft. A three-pronged approach can go a long way toward keeping a lid on risk.

**Employee Vetting**

Information collected during the hiring process generally helps hiring managers make informed and considered decisions. But without proper controls in place to see that background check processes are fully executed, the management team cannot be assured that any “problem” employees are filtered out.

Once candidates pass the screening process and are hired, they should be asked to sign employee contracts that include legally enforceable terms to protect critical business assets in cases of employee disputes or malfeasance. These terms should address:

- IP ownership
- Definitions of relevant IP
- Appropriate use and movement of IP data (including nondisclosure agreements)
- Restrictions on competition
- Sanctions for noncompliance
- Dispute resolution

It is not enough simply to have strong policies, standards and procedures in place; organizations also must communicate these requirements to employees. New-hire and annual training can help employees understand their responsibilities and rights.

**Vendor Contracting**

Organizations also must consider their contracts with vendors and other third parties involved in developing and manufacturing their products or services. The concepts outlined for employees apply equally to third parties.

These are some important questions organizations should ask on this front:

- Who has access to the organization’s critical IP?
- Who plays a vital role in developing and producing IP?
- Where do the third parties operate?
- Do those jurisdictions have IP requirements that are more stringent or less stringent?

**“AT A MINIMUM, ORGANIZATIONS SHOULD IDENTIFY WHAT THEIR IP COMPRISSES, WHO CONTROLS IT AND HOW IT IS PROTECTED.”**

Organizations must know the IP they are outsourcing when assessing vendor and collaborator risk and controls. At a minimum, organizations should identify what their IP comprises, who controls it and how it is protected. They also must closely scrutinize their IP licensing agreements to determine whether the agreements prohibit outsourcing of the IP without authorization.

While protecting IP rights in the United States is relatively straightforward, due to the strict enforcement regime built around such rights, it could become a greater challenge to enforce rights elsewhere. To avoid such hurdles, organizations need to establish controls to determine whether collaborators’ home countries are signatories of the various international IP protection treaties.
Border Controls
As with most areas of data security, the most critical (and logical) control points for IP data relate to the borders of an organization’s network. Controls around outbound email, permissible data transfer mechanisms, inspection of encrypted traffic and the use of cloud services are vital to preventing the theft of the low-hanging fruit of IP data. Implementing these controls can be easier said than done, but organizations should not leave these concepts out of a broader IP protection campaign.

Data Discovery
As organizations seek to better control their IP, it is necessary to understand the scope and usage of such data across the organization. This is a particularly daunting task for large organizations with many product lines, manufacturing facilities, international offices or vendor relationships, but no organization can protect an asset if it is unaware of the asset’s existence. This is where data discovery tools become crucial for managing IP.

These tools can come in multiple forms, such as passive network monitoring, active device scanning or user-based flagging. Data discovery tools that perform automatic scans to discover where data reside are included in numerous data loss prevention (DLP) tool sets and also are available as stand-alone products and services. In the coming years, advancements in machine learning techniques will yield new tools to help automate these discovery efforts, and some technology vendors already are moving in this direction. However, no magic bullet solutions exist at this point. Organizations need to select tools that are designed specifically to identify the types of data in which they are interested. This approach likely will result in the adoption of multiple tools to identify data across repositories such as databases, file shares, local files, email and cloud services.

Data Loss Prevention
Assuming that an organization has a strong grasp of the type of IP data it uses, how the data are classified and where the data reside on the network, it can use DLP technologies to further control the
data. DLP solutions come in several forms that address specific areas or technical components of IT infrastructure, including email, end points, cloud services or movement throughout the internal network. The appropriate tools will depend heavily on the organization’s specific areas of risk in terms of data format, movement and sensitivity.

**Revision and Source Code Control Systems**

IP data that take the form of source code or files that are subject to constant modification and revision should be managed and monitored by a version-control system. As with all sensitive IT systems, a version-control system should be accessible only by authorized personnel, hardened and subject to robust monitoring. Central repositories such as these often are complemented by the use of DLP technologies. Any anomalies regarding the movement of data or unauthorized modification should be investigated to preserve the confidentiality and integrity of IP.

**Getting Started**

For organizations that want to more effectively manage the security of their IP, the process should begin with a simple three-step approach:

1. **Identify.** Organizations must first identify and understand their data. Surveys can be a very useful tool to get the process rolling. By surveying employees from across the business, an organization can begin to understand the scope and complexity of its IP and then narrow the focus for more detailed conversations and evaluation. Examples of survey questions include:
   - How does your team define IP?
   - What are your thresholds for considering something sensitive?
   - Which form does the IP with which you work tend to take? Conceptual format? File format?
   - Do you tag or classify IP in any way?
   - What are the specific repositories used to store IP? File shares, databases, code repositories, etc.?

   An organization also can identify IP through the use of automated tools that can scan networks based on file type, file content (natural language processing), metadata or classification tags. The usefulness of these tools will depend on the form of the organization’s IP: The more IP takes a defined form or has consistent markers, the more effective the tools will be.

   For example, starting with a known, high-risk system such as a source code controls system, an organization can map the inbound and outbound data flows to understand other systems and networks that should be considered from a risk perspective. This will enable the organization to develop an understanding of the format of the data and ways in which they may be identified or tagged in the future.

2. **Control.** Once the organization’s IP data are better understood, the next step is to begin applying controls. Controls should be implemented based on risk and the business’s needs. Striking the balance between controlling the flow of data and allowing the business to operate efficiently and effectively always poses a challenge. A combination of management and technical controls (as previously outlined) should be considered and applied as appropriate.

   For example, an organization can start with low-hanging fruit for controls. It can terminate unnecessary data flows, encrypt all data flow channels going outside of the organization and review user access to the system. The organization can then continue to layer on controls to a level that allows the business to operate effectively while managing risk to an acceptable level.

3. **Evaluate.** Any control environment should be regularly evaluated to answer significant questions such as these:
   - Are the controls operating as expected?
   - Can a similar level of control be achieved with less friction?
   - Are the current controls aligned with new and emerging risk scenarios?
   - What feedback is being received from the business?
For example, an organization may choose to start by looking at past events and implementations of controls by performing audits or interviewing key stakeholders. This will help in trying to identify ways in which continuous monitoring, 100 percent testing or frictionless reporting can be integrated in the control strategy.

SECURING IP BEGINS WITH HAVING A DEEP UNDERSTANDING OF THE ORGANIZATION’S NEEDS AND GOALS, AS WELL AS THE RELATED RISK.

The Big Picture

Securing IP begins with having a deep understanding of the organization’s needs and goals, as well as the related risk. From there, management and technical controls can make great strides toward protecting the data. But organizations that seek peace of mind regarding the security of their valuable IP would be remiss to not also consider the nuances of employee management and international law.

Endnotes


7 Ibid.


Security in Depth

Over the past 25 years, the methodology of network security has changed almost beyond recognition. With the aggressive pace at which data have grown and the need for constant real-time access becoming the norm, paying increased attention to securing networks and data has become critical. As data become ever more available online and organizations are obliged to offer access to their information across a publicly mistrusted medium, the potential for and reality of data compromise have become very real. Organizations lose billions of dollars each year through this very phenomenon.

Security breaches seem to be a daily occurrence, one of the most recent being the Equifax breach, in which tens of millions of records were stolen. Although, at the time of writing, the actual cost of this breach remains unknown, it could easily approach the US billion-dollar mark. With this level of loss becoming a real risk, businesses are committing increasing amounts of resources to bolstering their data security. Such efforts have seen the movement to a layered defense model becoming the norm. Experts in the field are designing security measures so that information entering and leaving an organization must pass through several layers, in an effort to fill the gaps left by using a single security device. Some of these methods will be discussed in detail in this article.

Layered security is part of a larger strategy known as "defense in depth." Although these terms are sometimes used interchangeably, they are not the same. Defense in depth, which was developed by the US military as a policy and method of defense, is best described as: “A defense in depth approach to security widens the scope of your attention to security and encourages flexible policy that responds well to new conditions, helping ensure you are not blindsided by unexpected threats.”

Malware Defense

The prevention of malware is a significant factor when designing network security. How can one prevent malware from infiltrating the network? This pernicious software can be introduced in many ways. As an example, an email with a link prompting a user to download malware may be received; a user may mistype a web address and land on a rogue website designed to deliver malware; or a user may insert a malware-infected Universal Serial Bus (USB) stick into their computer. Once introduced, malware such as worm viruses can spread extremely rapidly to other unprotected, vulnerable computers and servers in the network.

With so many ways in which malware can enter a network, a single layer of protection is no longer sufficient. A popular method of layering defense against malware is to ensure that all data are scanned at least twice when entering and leaving the network.

To add another layer of protection, the scanning devices should be obtained from multiple vendors when possible. Malware protection typically works on signatures; using different vendors, with different signature databases, will fill in the gaps between signature update times to help protect against zero-day malware outbreaks. Security designers usually accomplish this goal by using malware protection end-point solutions for end-point scanning and layering these with email-scanning solutions and deep-packet malware scanning with a border device such as a firewall. This produces a multilayered scanning scenario. If someone sends an email to a user, the email is scanned for malware by the email scanner, then scanned again at the firewall level and then a third time by the end-point security software (figure 1). According to the US Federal Communications Commission, “The idea of layering security is simple: You cannot and should not rely on just one security mechanism to protect something sensitive. If that security mechanism fails, you have nothing left to protect you.”

Charles Hale, CCNA, CISSP, MCSE
Is the chief information officer for Legacy Healthcare, a US healthcare company. He has worked in information technology security for 15 years. Prior to working in the healthcare space, he provided security consulting to a broad spectrum of biotechnology companies ranging from small start-ups to publicly traded companies. Hale has a passion for technology and data security. He has committed his career to protecting sensitive data for data owners.
Restricting security to the implementation of a firewall alone is like locking the doors to a house with no alarm system.

It was once held that the implementation of a firewall at the border and the network would be enough. That methodology is no longer sufficient in today’s environment, where the untrusted network (the Internet) is a playground for hackers that is open 24/7. Restricting security to the implementation of a firewall alone is like locking the doors to a house with no alarm system.

Organizations need layered defenses at their borders, and the most effective way of obtaining that is through the use of both a firewall and an intrusion detection and prevention system (IDPS), preferably from different vendors so as to cover any vulnerabilities in the protection engendered by relying on a single vendor; any suspicious activity can then be reported (figure 2).

Firewalls may be extremely effective, but they cannot be relied on as the sole means of securing a network perimeter. In fact, the SANS Institute has determined this to be one of the seven most common mistakes made by management that jeopardize network security. Protecting the border, although a high priority, is not sufficient. Security needs to evolve from protecting the edge of the network from unauthorized access and malware into a layered security approach.
traffic only from the web server front end to the email database in the trusted network, thereby accomplishing the goal of layered security via network design. An IDPS will also scan the network traffic, creating yet another layer of security.

In addition to adding a DMZ segment at the network entry point, additional steps can be taken to section off high-priority assets on the network. For example, in the banking industry, typically at least one segment is used that possesses the highest level of security in the internal network. In industries with extremely high-risk assets, protecting the data from the outside is extremely important, as is protecting them from the inside. When customers go into a bank, they do not just see the cash sitting on the floor; rather, it is secured inside a vault, which creates another physical layer of security.

High-risk assets typically occupy their own segment, protected by another set of internal perimeter security devices. The security mechanisms may be firewalls or jump servers. Designers will create red (for low-security) and black (for high-security) zones. To move from a red to a black zone, in which high-priority databases reside, the user must go through a jump server. The latter first requires a Remote Desktop Protocol (RDP) session before accessing the database. This creates yet another layer of security in the network.

Proxy

An additional and valuable layer of protection that should be included in a comprehensive layering approach to security is the use of a network proxy or firewall proxy. A content filter at the network level is critical to the overall strategy. Proxies can filter out .exe or .bat files, which can greatly enhance the overall security package. Advanced filters can
also filter based on application type and reputation. These filtering databases are typically cloud-based and can be fast to respond to zero-day outbreaks of malware. They can also be highly effective at dealing with ransomware.

An application proxy acts as a gateway between the end-user system and the Internet, essentially hiding and protecting the end point. The user system makes contact with the application proxy, while the proxy communicates, on behalf of the user, with the external server. The latter never has access to the internal network. Although proxy systems alone are not a solution to security, they add a pleasing complement to virus protection and several other layers of network defenses.

Third-Party Networks

With security designers so concerned with preventing breaches and virus outbreaks in their internal networks, the security industry has responded by offering solutions that prevent potential malware from ever entering the end user’s environment. To complement the implementation of end-point security software and deep-packet scanning at the firewall level, many designers also use third-party networks to scan for threats before the traffic enters the end user’s network.

An excellent example of this is email scanning in the cloud using a vendor network. Several vendors offer this service, including Barracuda and Apprizer. The design requires email sent to the end user to be diverted to the third-party network, where it is scanned for viruses, phishing, spam or many other combinations of filters. Any potential threats are removed before the clean email is sent to the end user’s internal servers. These security solutions are extremely granular and very quick to respond to outbreaks.

An added benefit of this service is that traffic bound for the internal email server is reduced significantly. According to statistics, more than 69 percent of emails sent in 2013 were either spam or viruses. The number of spear-phishing email campaigns increased by 91 percent in 2013 over the year before, indicating that attackers had become more sophisticated in their assaults. They are learning about the end users and targeting specific individuals deemed to be high-value targets. With that type of statistic, the added layer of passing the Internet traffic through a third-party network where the traffic can be scanned for threats is of high value in a layered-security approach (figure 3).

Physical Security

Although the need for physical security may seem obvious, it can all too easily be overlooked. It makes no sense to have a layered approach to network security and neglect the physical aspect. Physical security is not merely a layer of network security; it needs to be layered in its own right. For example, one key that allows access to the server room, or one camera that records entry to the building, is not sufficient. Access to the building should be restricted and monitored, just like the network infrastructure. If someone compromises the network from the outside, the organization’s mechanisms should alert employees and allow them to establish what information was compromised and for how long.

Physical security should serve the same purpose: If someone compromises the physical security, resources should be in place to tell who breached the defenses, where and when. This is done by deploying security guards where possible and having keyed and logged access to the building, including separate access to sensitive areas such as the data center. Access to the building should be recorded via a camera system, while a separate system should monitor access to sensitive areas.

These components, just like network logging, should be reviewed on a regular basis. It is not advantageous to have cameras in place if no one is reviewing them, nor to have electronic card access.
Every authentication system can be compromised and should not, particularly those with high-value assets (e.g., banks, power plants), rely on a single form of authentication.

Designers can use several options to achieve MFA. These can be broken down into three categories: something one knows (a password), something one has (a token number or code sent via email or text), or something one is (biometric). Security designers combine two or more of the three categories to create MFA. The procedure is effective only when the logs are not evaluated. Alerts should also be configured to rouse security personnel regarding any failed attempts to access the building or sensitive areas. In sum, physical security is a key component of a layered security implementation.

**Authentication**

Authentication is the process of proving that people are who they say they are. This procedure is at the core of every security system in use today. As discussed in this article, these systems have layers of protection to keep people who are not meant to be there, or to have access, out of the network and away from data. These processes cover the back doors and prevent the infiltration of malware. Authentication is the process of allowing permitted access through the front door of a network. This operation must also be layered, just like other sections of the network. How is this accomplished? By using multifactor authentication (MFA). "The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network."12
two or more passwords are required. For example, a person accessing a financial database may be required to enter a password (something he/she knows), then enter the code from a smart card (something he/she has), and may still be required to scan a fingerprint or iris for access. Following this process allows for layered security during authentication.

**User Education**

With the increase in social engineering and zero-day attacks, user education plays a huge part in a layered security approach. The end user may be the final or first (depending on where the attack originates) line of defense. To ignore the user would be a massive mistake. With script kiddies becoming more prevalent, these amateurs can easily circumvent firewalls by sending mass emails in an attempt to persuade users to click on loaded links; the user must be aware of the risk. According to one expert:

_A strong security architecture will be less effective if there is no process in place to make certain that the employees are aware of their rights and responsibilities. All too often, security professionals implement the 'perfect' security program and then forget to factor the customer into the formula._

**Testing**

The final step in any sound security design is the testing phase. Routine testing should be a matter of written policy and followed to the letter; network security officers should look at themselves as military personnel and be constantly prepared for an attack. Building defenses, setting alarms and monitoring is not enough—it is necessary to constantly test the defenses. Such testing must be performed both internally and externally, by internal staff and outside security experts. “Penetration testing is like having a mock firefight on a military base.” White-hat hacking, penetration testing and vulnerability testing are crucial in a layered security approach to network defense.

**Conclusion**

With the increase in data breaches and the resultant cost to organizations, the protection of networks and data is paramount. Firms cannot afford to turn a blind eye to network security. Organizations are increasing their security spending, and in many cases these additional resources are going to add layers of defensive mechanisms.

Security designers are using various approaches to layering defenses to thwart hackers and prevent data loss. They are implementing layers to prevent malware infections and head off hackers at the border, and increasing the complexity of network design to add additional passes through checkpoints for data access. Designers are also routing traffic through third-party security networks before entry into the trusted network to weed out threats before they ever enter the network.
Those in charge of physical security, meanwhile, are implementing layered security in their design and complementing network-based layered security. The process of MFA is quickly becoming de rigueur in the move to standardize the process of a layered defense. Security officers are educating their user base as well as using mechanisms to test the effectiveness of their programs.

Policy design and implementation are crucial in designing and implanting layered security. The security policy of modern networks is to mandate many layers of data scanning before entry and/or exit from the network. Although these methodologies will not prevent all data loss, with the concept of layered security becoming the norm, they will play a significant role in protecting the networks of today and tomorrow.

Endnotes
10 Ibid.
14 Op cit Choi et al
Active Defense

Every year, ISACA® conducts its annual Global State of Cybersecurity research.¹ The second part of the survey asks about security practices in the field: what is working and what is not. No need to spoil it for readers (who will have to wait for the report to come out for the specifics), but this year there were interesting findings when respondents were asked about active defense. Specifically, active defense methods are used more frequently than one might think—and they are highly effective when they are used.

What Is Active Defense?

Like many things in security, active defense—as a term—is borrowed from defense terminology. Specifically, it refers to actions taken to deny a position, resource or other advantage to an adversary. In the context of cybersecurity, it refers to measures that can be taken to actively disrupt or interfere with an attacker’s campaign against an environment. For example, if a security team were to install a honeypot and load it with juicy-seeming (but fake) documents to actively waste the attacker’s time, that would be an active defense strategy.

It bears noting here that I do not mean “hacking back” for the purposes of this discussion.

Sometimes, there is confusion about the distinction between “active defense” and so-called “hack back” strategies. In my opinion, active defense is designed to disrupt an attacker’s activity through minimally-invasive and clearly delineated strategies. By contrast, “hacking back”—for example, by attempting to scan, penetrate or gain entry into an attacker’s environment—is (again, in my opinion) both ethically and potentially legally problematic. So, if there was any confusion before, let it be clear now that this discussion refers throughout to active defense strategies and not attempting to “hack the hackers.” Specifically, it refers to things that either:

• Waste the attacker’s time
• Trap and contain attacks
• Alert security teams to attacker activity so it can be monitored
• Help with attribution and discovery

There are a few reasons why active defense can be a particularly useful and effective strategy. First and foremost, it can help to disrupt an attacker’s campaign. As we know from looking at adversary activity as a life cycle (i.e., as a “kill chain” that starts with reconnaissance, proceeds to infiltration and lateral movement, and ends with exfiltration or some other equally undesirable outcome) any interruption in the attacker’s ability to proceed from phase to phase can cause the overall campaign to fail. Likewise, there is “dwell time” of which to be conscious; the campaign has a window of time between when it is initiated and when it is discovered. Anything that can frustrate attackers’ ability to realize their outcome increases likelihood that the attack can be detected and stopped within that window before the attackers are successful.

In addition to that, though, active defense can also assist with attribution. This is particularly useful from a law enforcement point of view; for example, it can support criminal proceedings against someone or warn others of an attacker campaign or tradecraft. In other words, if an organization identifies or can establish who is responsible for attempting an attack, it is useful information that can be passed along to law enforcement.

Ed Moyle

Is a founding partner of the analyst firm Security Curve. Prior that, Moyle was director of thought leadership and research at ISACA. In his nearly 20 years in information security, he has held numerous positions including senior strategist with Savvis, senior manager with CTG’s global security practice, vice president and information security officer for Merrill Lynch Investment Managers. Moyle is coauthor of Cryptographic Libraries for Developers and a frequent contributor to the information security industry as an author, public speaker and analyst.

¹ The second part of the survey asks about security practices in the field: what is working and what is not. No need to spoil it for readers (who will have to wait for the report to come out for the specifics), but this year there were interesting findings when respondents were asked about active defense. Specifically, active defense methods are used more frequently than one might think—and they are highly effective when they are used.

https://bit.ly/2ib0huk
Tools
With this in mind, there a few free tools to consider when looking to get familiar and just play around with active defense strategies. Like any security tool, practitioners do not want to just field these willy-nilly, but instead, for a production deployment, with care and strategic foresight. That said, it is always helpful as a starting point to kick the tires and gain familiarity.

WebTrap is small, recent and very targeted. It lets the practitioner mirror an existing web page (e.g., a corporate information portal or project page) and alert (e.g., via a syslog event) when someone interacts with it. That said, any web server can be customized for this purpose by mirroring an internal page and setting up custom reporting when it is accessed.

One of the better starting points is a honeypot. A relatively versatile one to tinker with—and one that is well documented from a usage standpoint—is OpenCanary (https://github.com/thinks/opencanary). OpenCanary makes a good starting point because, conceptually, it is fairly simple: It runs services and triggers when someone connects to them. The services in question are designed to emulate a particular device configuration (e.g., a Windows or Linux server).

There are, as one might imagine, literally dozens of other open-source honeypot options to choose from and, depending on what type of service or environment practitioners want to emulate, there are plenty of choices available (a helpful list can be found here: https://github.com/paralax/awesome-honeypots#honeypots). It is, of course, useful to select a honeypot that resonates with an environment. For example, if one is running a 100 percent Windows shop, a Secure Shell (SSH) honeypot designed to mimic a Linux web server might seem out of place. Ideally, one that will blend in with services already in use should be selected. Another option to consider is WebTrap (https://github.com/illusiveNetworks-Labs/WebTrap).

Taking the honeypot concept one step further is HoneyBadger v2 (https://github.com/lanmaster53/honeybadger). HoneyBadger includes a framework for geolocation—helping to pinpoint where the attacker is located. This can help bolster attribution capability by providing information about the location from which the remote attacker is coming. Used in combination with a tool such as Molehunt (https://github.com/Prometheaninfosec/Molehunt), one can get a fairly clear picture of who is attacking and the attacker’s location since Molehunt allows the user to create documents that, when opened, let security teams know about it. One might, for example, deliberately allow a document to be exfiltrated and, together with HoneyBadger, glean attribution-relevant information about the person opening it. Again, this tool is minimally intrusive and solely focused on information gathering and assisting law enforcement.

The last approach discussed here is the Browser Exploitation Framework (BeEF) (https://beefproject.com/). BeEF is arguably more of a penetration testing tool than an active defense tool, but it bears mentioning because it can, in certain circumstances, be used to support active defense as well. First, it is important to note that it is imperative to use this tool in a lawful way. If there are doubts about whether an approach is lawful, it should be discussed with the legal team. If a user cannot determine if the planned usage is lawful, it should be discussed with the legal team. If a user cannot determine if the planned usage is lawful, it should be discussed with the legal team.

Endnote

ISACA JOURNAL VOL 3 53
Blockchain technology is being considered by many organizations, such as those involved in banking and finance, supply chain, and logistics, for applications that involve multiple users and multiple transactions in a distributed environment. Many banks have initiated projects to develop solutions using blockchain technologies. Other applications that are being considered include SDP and asset management, identity management, and supply-chain management. Financial organizations, particularly banks and security markets, are collaborating with developers to create financial technologies (FinTech).

Risk management for solutions developed using blockchain or distributed ledger technology (DLT), therefore, must be considered for different objectives related to governance, processes, operations and resources, including human resources. In the case of Bitcoin and other digital currencies, recent events have indicated that the absence of a central governing body has created concerns as no party is responsible or accountable for the proper operation of the system that may represent risk to user organizations.

Many market participants are working to develop solutions using private blockchain networks, in which implementing a governance structure can be managed as the participants are trusted parties.

The risk associated with blockchain technologies is similar to the risk associated with other technologies and current business processes, with some small differences for which organizations need to consider appropriate risk vs. benefits. Risk management for any technology-based application requires understanding of three aspects:

1. Organizational objectives related to benefit realization for deploying the application
2. Factors that will introduce uncertainties (e.g., threats and vulnerabilities) in achieving objectives
3. Cost associated with implementing controls to mitigate the risk
Based on these aspects, one can approach the risk management solution for blockchain-based applications. The following areas may be considered for risk management:

- **Strategic**—The technology must be considered a priority:
  - Leadership—Should the organization wish to take lead and invest in new technologies or should it wait until those technologies mature? The decision depends upon the organization’s risk culture and risk appetite.
  - Transparency—Should the system be an open network, like digital currencies, or closed within strategic business partners?

- **Continuity**—Considering the nature of technology and the related complexities, the organization needs to consider the risk associated with continuity.

- **Transformation**—There is risk associated with implementation. Current business processes will need to undergo change and organizations need to consider how the changes are going to affect historical data.

- **Reputation**—The failure of new technology may result in materializing risk associated with loss of reputation.

- **Information security:**
  - Technology—Blockchain technology is said to be secured since it uses encryption. However, risk associated with the encryption technology and key management has to be addressed.
  - Systems and processes—Risk due to process control failures needs to be considered. Incidents related to Bitcoin are due to the failure of controls in these areas.
  - People—Humans are the weakest link in security. Collusion and social engineering particularly can result in security incidents.

- **Regulatory noncompliance**—Because blockchain is a new technology, regulators are cautious about its use. Depending upon the nature of the use cases, regulatory compliance must be considered while developing and using the technology. Consideration must also be given to cross-border data transmission and regulations related to anti-money-laundering.

- **Operational**—Current policies and procedures need to be revisited to meet the requirements of the new technology.

- **Contractual and supplier**—Considering collaboration between multiple parties and vendors, there need to be appropriate service level agreements (SLAs) between administrators and participating organizations.

- **Confidentiality of data**—Since all participating organizations have access to the records and data, the risk associated with confidentiality of data needs to be considered. This is also linked to regulatory compliance.

- **Privacy of data**—As with confidentiality of data, privacy of data is an important aspect that needs to be evaluated before implementing blockchain technology.

Blockchain technology is still new, but it is likely to transform current business methods that may expose organizations to new risk, challenges and competitive advantages/disadvantages. Organizations should establish an appropriate risk management strategy, effective governance and use of a controls framework.

**Author’s Note**

The views expressed here are generic and based on available information and should not be considered as complete guidance on this topic.

**Endnotes**

6. Ibid.
7. Op cit Financial Industry Regulatory Authority
Correction notice: Due to an error, the print version of the ISACA® Journal vol. 3 contains an incorrect version of the Crossword Puzzle clues. That error has been corrected in this online version of the Crossword Puzzle. We apologize for the error and the inconvenience to readers.

ACROSS
1. Changing to a new system
5. Important credential for IS audit professionals
8. Unsusceptibility
9. Instrument created for a particular purpose
10. Unfortunate
11. Protocol for file transfers
13. Methodical examination
14. Incident
15. Atmosphere or ambience
16. The entire range
17. Conditional word
20. Weigh
22. The R in RFID
23. Benchmark, abbr.
25. Right of an individual to trust the appropriate storage and use of personal information
27. Transfer back to the original country where business was being physically controlled
30. Russia’s Internet domain
31. Nimbleness
33. Initial step in project development
36. Collect data covertly
37. Effort to rationalize disparate and overlapping databases to ensure the accuracy, integrity and consistency of corporate data
38. Encryptioning ransomware

DOWN
1. AKA CPU
2. Rare find
3. Yearly
4. Believer suffix
5. They must always be checked before granting access
6. Sudden rise
7. Authenticate
9. Leonardo’s middle name
10. Dumbfounded
12. One of the words in a major health insurance act
16. Courageous
18. Expose oneself to a chance of injury or loss, 3 words
19. Officer responsible for information security, abbr.
21. Alien flyer
24. Party
25. Strategizes
26. Reduce, as a budget
28. Trendy
29. ___ command
32. Edible tuber
33. Cell phone’s smart card
34. Bank account abbreviation
35. US government procurement overseer, abbr.

Answers on page 58
TRUE OR FALSE

SOOD AND JALIL ARTICLE

1. IT departments that wish to understand potential cloud threats must have visibility into the data flows between users and cloud apps that exist outside the network and perimeter security defenses.
2. Of all the attack methods deployed by malicious actors to steal credentials and hijack accounts, phishing is the least commonly used.
3. The difference between man-in-the-browser and man-in-the-cloud attacks is that the former steals tokens and the latter steals account credentials.
4. Among the countermeasures to defend against threats to cloud applications (apps) are scanning files when they are uploaded to and downloaded from the cloud, using behavior modeling and analysis to discover anomalies in user behavior while they are interacting with cloud apps, enforcing policy and using a cloud app security solution for compliance purposes.

VAN STONE AND HALPERT ARTICLE

5. A good example of corporations’ recognition of the significant risk inherent in protecting data is the list of risk factors included in Alphabet Inc.’s 31 December 2016 10-K, of which 50 percent deal with data security risk.
6. Real-life losses of data have occurred from such unintentional acts as loss of a mobile phone, return of a leased photocopier without wiping the data stored on the machine, a stolen laptop and clicking on email malware.
7. Anti-malware has remained a very effective defense over time because malicious actors have been unable to develop hacks to evade common malware tools.

MARAJU ARTICLE

8. Expert systems are artificial intelligence systems that review security code and offer code review guidance through forward and backward chaining.
9. Cross-site scripting (XSS) results from improperly validating (for malicious inputs) the input data submitted to a web application. Despite the improper validation, however, XSS does not constitute a security vulnerability.
10. Structured Query Language (SQL) injection vulnerability attacks occur when attackers inject malicious SQL commands to the backend database and exfiltrate database details.

KHAN ARTICLE

11. Research indicates that approximately half of the American population can be uniquely identified by their gender, ZIP code and birthdate.
12. Anonymization is essentially the destruction of identifiable data, making it impossible for anyone to establish the identity of the data. It also makes it virtually impossible to reestablish the data together.
13. Pseudonymization is sometimes accomplished by eliminating all identifying data elements and replacing them with an internal numerical identifier, which makes reidentification impossible for a third party but easy for the data controller. As such, such identifiers are not considered personal data.
14. Permutation alters data attributes by randomly adding values to or subtracting values from the existing personal data.

CLARK ARTICLE

15. Machine learning is used by businesses for competitive advantage, giving them ways to optimize operations and develop new services. This usage establishes a need for machine learning audits. Fortunately, an accepted procedure for how to perform such an audit is in place.
16. Auditors can assess the efficacy of a specific machine learning algorithm by examining a domain-specific, modified version of the software development life cycle.
17. Frameworks for auditing machine learning algorithms exist (e.g., LIME and FairML), but they interpret only the model weights and do not provide a risk-based, holistic understanding of the machine learning process.
18. Any machine learning audit must include an examination of whether or not the data were bifurcated into training and test sets.

AKANNI ARTICLE

19. High levels of volume, velocity and variety are what make big data big.
20. The form in which the data were generated and the rate at which they were generated constitute challenges to using big data. However, the biggest challenge is the cost to store the data.
21. Many cloud service providers (CSPs) use Software as a Service (SaaS) to implement big data, breaking the related activities down into enablement, integration and testing phases.
TRUE OR FALSE

Sood and Jalil Article

1. 
2. 
3. 
4. 

Van Stone and Halpert Article

5. 
6. 
7. 

Maraju Article

8. 
9. 
10. 

Clark Article

11. 
12. 
13. 
14. 

Khan Article

15. 
16. 
17. 
18. 

19. 
20. 
21. 

Answers: Crossword by Myles Mellor
See page 56 for the puzzle.

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 +1.847.253.1755. 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, 1700 E. Golf Rd., Suite 400, Schaumburg, IL 60173 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, CRISC, CISM or CGEIT CPE credit.
ISACA Member and Certification Holder Compliance

The specialized 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 mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment 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 Organizational 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 categorization as the standards (also divided into three categories):

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

General

2001 Audit Charter
2002 Organizational 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, Thought Leadership and Research, via email (standards@isaca.org); fax (+1.847.253.1755) or postal mail (ISACA International Headquarters, 1700 E. Golf Road, Suite 400, Schaumburg, IL 60173, 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.
Is Your Enterprise Ready for the GDPR Compliance Deadline?

**WHO:** Enterprises that offer goods or services (regardless if payment is required) within the EU as well as enterprises that monitor EU subjects’ behavior within the EU.

**WHAT:** New data privacy mandates have been issued by European Union regulation.

**WHERE:** Includes any organization in the world if it retains or processes information on any citizen in the EU.

**WHEN:** GDPR compliance must be achieved by 25 May 2018.

**WHY:** To better protect any individual’s personal information, to secure rights for the individual over that collected information, and to force enterprises to follow a uniform scheme for data protection.

**HOW:** Follow ISACA’s privacy guidance on how best for your enterprise and its staff to assess your unique data protection needs and meet the GDPR compliance standards set by the EU.

**ISACA-CMMI GDPR ASSESSMENT**

ISACA-CMMI’s complimentary tool, *GDPR Assessment*, provides users with a roadmap for GDPR implementation based on the answers to a series of questions/statements. The resulting customized assessment offers insights as to where your organization should focus its data protection efforts. Over time, as your enterprise’s GDPR implementation moves forward, users can retake the assessment to gauge progress on compliance.

The *GDPR Assessment* is powered by the expertise of both ISACA and CMMI. For nearly 50 years, ISACA has supported the global IS/IT community with world-class guidance in the areas of privacy and security. For more than 25 years, CMMI has helped enterprises evaluate performance and maturity through their scoring practices models.

This tool is a valuable resource for data protection officers (DPOs); security, compliance and audit executives and managers; data privacy authorities and their auditors; as well as consultants, external auditors and assessors.

[www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-CMMI-GDPR-Assessment.aspx](www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-CMMI-GDPR-Assessment.aspx)
Implementing the General Data Protection Regulation

As of 25 May 2018, all enterprises that conduct business and hold personal data on just one person located in the European Union will fall under the mandates of a new EU requirement—the General Data Protection Regulation (GDPR). All EU businesses are subject to GDPR, but its effect goes even farther. Given the global scope of today’s digital-based commerce, the impact of GDPR certainly will be felt by many businesses across the world and located outside the physical borders of the EU.

Undertaking monumental compliance changes to organizational data protection strategy and information security requires trustworthy, comprehensive guidance. ISACA’s new guide, Implementing the General Data Protection Regulation, was created to address the many data protection and privacy concerns found within commercial and not-for-profit enterprises. From C-suite to legal and IT teams, from operations and vendor management to marketing and communications, this reference provides valuable information on GDPR readiness, assessment and compliance.

Print Product Code: GDPR
Member Price: $40.00
Non-member Price: $80.00
Web Download Product Code: WGDPR
Member Price: $25.00
Non-member Price: $50.00

ISACA Privacy Principles, Governance and Management Program Guide

The main purpose of ISACA Privacy Principles, Governance and Management Program Guide is to provide readers with a harmonized privacy framework. The book offers a set of privacy principles that align with the most commonly used privacy standards, frameworks and good practices, as well as fill in the gaps that exist among these different standards. This practical guide can support or be used in conjunction with other privacy frameworks, good practices, and standards to create, improve and evaluate a privacy program specific to the practitioner’s enterprise. Special guidance on how to use the COBIT 5 framework to implement a more robust privacy program is included in this publication.

Print Product Code: IPP
Member Price: $45.00
Non-member Price: $90.00
Web-download Product Code: WIPP
Member Price: $35.00
Non-member Price: $70.00

Implementing a Privacy Protection Program: Using COBIT 5 Enablers with the ISACA Privacy Principles

Privacy breaches can cause a cascade of negative impacts on enterprises, as well as significant harm to the associated data subjects. Enterprises may suffer financial loss and reputational damage, be charged with failure to comply with regulations and legislation, and alienate key stakeholders who demand safety of personal information. To avoid these outcomes, enterprises must establish and maintain a formal privacy protection program. This publication shows how to optimize a privacy program built on the framework of COBIT® 5 through focused, yet comprehensive, application of its enablers.

Print Product Code: IPP2
Member Price: $60.00
Non-member Price: $100.00
Web Download Product Code: WIPP2
Member Price: $50.00
Non-member Price: $90.00
Blockchain Fundamentals

Blockchain has the potential to become a major force for innovation and change the way you process everything with records—from registrations, records of ownership, transfers of value and stock purchases, to identities and healthcare. The current digital world is built on ledger systems that worked well in past generations, but that fail to provide you with the capability to address the ledgers that are needed in an Internet-driven world. The basic blockchain characteristics that successfully create a secure and trustable infrastructure to support the Bitcoin cryptocurrency system are disrupting how we create and use ledgers, which, in turn, has the potential to bring significant value to the global economy and provide new capabilities that enhance government and business functions. Blockchain use is not limited to cryptocurrencies. Other blockchains are being developed so that input and output transactions contain ledger entries for numerous other items, including financial instruments, public records, contract information, other items demonstrating ownership or professional capability, and identities. Using trusted technologies to create its unique structure, blockchain features—such as openness, decentralized infrastructure, ability to transact anonymously while ensuring identity, and elimination of third-party attestation.

Web Download Product Code: WBCB
Member price: $25.00
Non-member price: $50.00

Guide to China’s Regulatory Cybersecurity Implementation Framework

China solicited public comment on the Cybersecurity Law of the People’s Republic of China (National Cybersecurity Law) beginning on 6 July 2016, and the law formally came into effect on 1 June 2017. The National Cybersecurity Law is China’s fundamental law pertaining to the cyber security domain and is of landmark significance as it is the first to be published in which cyber security requirements have been specifically codified in legal form for China. It defines the responsibilities of the country, government authorities, network owners, operators and ordinary users; it stipulates penalty provisions for breaches; and possesses stronger powers of execution than any other single collection of security specifications.

Web Download Product Code: WGIC
Member price: $30.00
Non-member price: $60.00


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, data, and security implications of evolving technology.

This 2nd Edition accounts for the rapid changes to our global security landscape. It takes a deeper dive into cyberrisk and risk identification, with material from ISACA’s CRISC Manual. It also includes updated information on cybersecurity concepts, such as ransomware, policies and cybersecurity controls. Architecture principles are updated to consider web application firewalls, SIEM solutions and revised encryption applications. Network security sections are updated to include access controls, wireless network protections, and tunneling. Evolving technology now includes security implications of the internet of things, big data, artificial intelligence and social media.

Print Product Code: CSXG2
eBook Product Code: EPUB_CSXG2
Member price: $60.00
Non-member: $65.00
Web Download Product Code: WCSXG2
Member price: $50.00
Non-member price: $55.00
Securing Mobile Devices

Securing Mobile Devices should be read in the context of the existing publications COBIT 5 for Information Security, Business Model for Information Security (BMIS) and COBIT 5 itself. This publication is intended for several audiences who use mobile devices directly or indirectly. These include end users, IT administrators, information security managers, service providers for mobile devices and IT auditors.

The main purpose of applying COBIT 5 to mobile device security is to establish a uniform management framework and to give guidance on planning, implementing and maintaining comprehensive security for mobile devices in the context of enterprises. The secondary purpose is to provide guidance on how to embed security for mobile devices in a corporate governance, risk management and compliance (GRC) strategy using COBIT 5 as the overarching framework for GRC.

Implementing the NIST Cybersecurity Framework

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.

Controls and Assurance in the Cloud: Using COBIT 5

This book provides practical guidance for enterprises using or considering using cloud computing. It identifies related risk and controls and provides a governance and control framework based on COBIT 5, and an audit program using COBIT 5 for Assurance. This information can assist enterprises in assessing the risk and potential value of cloud investments and determine whether the risk is within the acceptable level. In addition, it provides a list of available publications and resources that can help determine if cloud computing is the appropriate solution for data and processes in scope.
THE EXPERTISE FOR WHAT’S NEXT.
THE TRAINING YOU NEED, NOW.

• Interact with experienced ISACA® or Deloitte instructors who are experts in their field.
• Save time with focused Training Week courses offering hands-on learning.
• Earn up to 32 CPEs at each 4-day course toward certification maintenance and develop real-world skills you can apply immediately.

Develop career-enhancing expertise that can help shape your future role.

SEE WHAT’S NEXT, NOW

REGISTER TODAY AT ISACA.ORG/TRAINING18JV3

PREPARE FOR YOUR NEXT ROLE, NOW.
Gain new tools and techniques as you advance or refresh your knowledge.

ISACA TRAINING COURSES

TUITION:
ISACA Members US $2,295 | Non-Members US $2,495

- CISM Bootcamp: 4-day Exam Prep
- COBIT 5: Strategies for Implementing IT Governance
- Cybersecurity Fundamentals 4-day Cram Course
- Foundations of IT Risk Management
- Fundamentals of IS Audit & Assurance
- Governance of Enterprise IT

ISACA/DELOITTE TRAINING COURSES

TUITION:
ISACA Members US $2,495 | Non-Members US $2,695

- Cloud Computing: Seeing through the Clouds—What the IT Auditor Needs to Know
- Healthcare Information Technology
- Information Security Essentials for IT Auditors
- Analytics & Automation in Action: Utilizing Data Analytics & Automation to Enable Internal Audit
- An Introduction to Privacy and Data Protection
- Network Security Auditing
- Taking the Next Step—Advancing Your IT Audit Skills

For details on discounts, deadlines, registration, cancellation and more, VISIT ISACA.ORG/TRAINING18JV3
CYBER SECURITY TRAINING
JUST GOT REAL

NOW YOUR STAFF CAN COMBAT REAL THREATS IN REAL TIME TO BUILD REAL TECHNICAL SKILLS.

Yesterday's lecture-based cyber security training won’t protect your organization against tomorrow’s advanced cyberthreats. That’s why ISACA’s new Cybersecurity Nexus™ (CSX) Enterprise Training Platform offers your security team:

- On-demand access to 200+ hours of training for less than the cost of one typical course
- Practical, hands-on training labs performed in a live, dynamic network environment
- Continually updated content based on the latest real-world threats and scenarios
- Performance-based assessment of current and prospective employees’ technical skills

SCHEDULE A DEMO OF THE CSX TRAINING PLATFORM AT WWW.ISACA.ORG/CSXCYBERTRAINING