

# ISACA, UNE SOURCE D'INFORMATION INCONTURNABLE EN CYBERSÉCURITÉ

DAVID HENRARD, CISA, CISM, CRISC

# LA PLATEFORME CSX

## HTTPS://CYBERSECURITY.ISACA.ORG/



ENTERPRISE TRAINING

SHARE

SEARCH

LOGIN

MENU

## GAINED NOT GIVEN

Experience and judgment. Strength and momentum. Confidence and trust. They're all gained by the things we accomplish. And like anything truly valuable, they're never just given. Cybersecurity Nexus™ (CSX) is a new program designed for the most ambitious cyber security professionals, empowering them to elevate their work, take control of their career paths and earn their place amongst the best.

LEARN MORE

DISCOVER CSX



### JOIN THE BEST OF THE BEST

Unlock the full potential of your Cybersecurity Nexus experience and elevate your career by becoming a member of ISACA.

BECOME A MEMBER



### GET CERTIFIED. GET NOTICED.

Prove your place among the industry leaders and advance your career by earning a performance-based CSX Practitioner certification.

GET CERTIFIED



### LAY THE FOUNDATION.

Launch your career by exploring the industry standards, guidelines, and practices with our Cybersecurity Fundamentals Certificate.

ENROLL TODAY



# DES ACTUALITÉS

**CSX**  
CYBERSECURITY NEXUS

ENTERPRISE TRAINING | SHARE | SEARCH | LOGIN | MENU

Home > Latest News

## LATEST NEWS

Filter By: News Type | Sort By: Most Recent

1 - 10 of 26

**Overcoming the cyber-security skills gap: experience vs qualifications**  
SC MAGAZINE UK | by Danielle Correa | March 2017  
Experience is gaining importance over degrees and certifications.

**Security Think Tank: Governance framework key to best security at lowest cost**  
COMPUTER WEEKLY | by Maxine Holt | March 2017  
How to maintain operations at low costs, without security compromise

**Cloud security still a work in progress**  
NETWORK WORLD | by Jon Oltsik | March 2017  
Suggestions for gaining the right skills for cloud security

**Secrets of a Highly Productive CIO-CISO Relationship**  
INFORMATION WEEK DARK READING | by Kelly Sheridan | March 2017

**FEATURED NEWS**

*Fighting Cyber Security F.U.D. and Hype*  
NEWS ARTICLE

*What's the value in attack attribution?*  
NEWS ARTICLE

*Understanding the attack surface to better allocate funds*  
NEWS ARTICLE

# UN SUIVI DES MENACES ET VULNÉRABILITÉS



Get ahead of the threats and vulnerabilities that today's organizations are facing with our cyber security feed. Check back to see additional resources as new content is made available.

07  
APR  
2017

## Baseband Zero Day Exposes Millions of Mobile Phones to Attack

03:10 PM EST

A previously undisclosed baseband vulnerability impacting Huawei smartphones, laptop WWAN modules and IoT components was revealed Thursday at the Infiltrate Conference

07  
APR  
2017

## Creating a More Altruistic Bug Bounty Program

01:22 PM EST

David Jacoby and Frans Rosén said at this year's Security Analyst Summit they offered companies free pen-testing and raised \$15,000 for charity in the process.

ADVERTISEMENT

**Build Your Enterprise Skills Base — Train for Your Specific Needs On-Site**

[LEARN MORE >](#)

# DES WEBINAIRS



Register ahead of time for each month's Cybersecurity Webinar, presented live by subject matter experts, or check out archived webinars, both accessible to you free of charge.

## UPCOMING WEBINARS

25  
APR  
2017

### Aligning Awareness to NIST's Cybersecurity Framework

1H | by Tom Pendergast, Ph.D. | 11:00 AM (CDT) / 16:00 (UTC)

NIST's Cybersecurity Framework has become the de facto standard for structuring a cybersecurity program. Industry analyst Gartner has projected that 50% of U.S. organizations will use the framework by 2020. But how can the Framework be used to inspire a world-class security awareness program? In...



## ARCHIVED WEBINARS

ADVERTISEMENT



# LA DESCRIPTION DES MENACES

**THREATS (10)**      **CONTROLS (72)**

Sort By:       View By:  

<p><b>APT</b></p> <p>Advanced Persistent Threats (Generic) The term “advanced persistent threat” (APT) denotes a type of threat and attack that is technically sophisticated and usually present in the context of...</p>	<p><b>CYBERCRIME</b></p> <p>Cybercrime (Generic) The term “cybercrime” includes a wide range of criminal acts directed at individuals or enterprises. The specific background to calling a criminal act a “cybercrim...</p>	<p><b>DDOS</b></p> <p>Distributed Denial of Service (Generic) The term “denial of service” generally denotes an attack, or series of attacks, on an IT environment, with a view to disrupting or disabling the services p...</p>	<p><b>INSIDER THREATS</b></p> <p>Insider Threat (Generic) An insider threat is defined as the potential of an adverse act or omission from within the organization, i.e., committed by employees or individuals with a spec...</p>
<p><b>MALWARE</b></p> <p>Malware (Generic) The term “malware” denotes any malicious software used for the purpose of attacking systems and IT environments. There is a vast numbe...</p>	<p><b>MOBILE MALWARE</b></p> <p>Mobile Malware (Generic) Mobile malware denotes a specific type of malware that affects mobile devices, most notably smartphones. The emergence of mobile malware has b...</p>	<p><b>RANSOMWARE</b></p> <p>Ransomware (Generic) The term “ransomware” denotes the insertion of malware that is designed to extort a ransom in money or money equivalent from the end user. This is usually ach...</p>	<p><b>SOCIAL ENGINEERING</b></p> <p>Social Engineering (Generic) The term “social engineering” incorporates any and all human-intelligent interactions that are designed to elicit an involuntary or unconscious response...</p>
<p><b>UNPATCHED SYSTEMS</b></p> <p>Unpatched Systems (Generic) Unpatched systems are programs for which a patch—software that modifies a system, application or other program—is either unavailable or ha...</p>	<p><b>WATERING HOLE</b></p> <p>Watering Hole (Generic) The term “watering hole” denotes a technique whereby end users visiting a certain web site are covertly redirected to another web site that will deliver ma...</p>		

# LA DESCRIPTION DES CONTRÔLES

**THREATS (10)** | **CONTROLS (72)**

Filter By: Category Threat Sort By: Category A-Z View By: [Grid] [List]

1 - 12 of 72 | View: [12](#) [24](#) [36](#) [48](#) [60](#) [ALL](#) [1] [2] [3] [4] [5] [8] [NEXT »]

<b>ARCHITECTURE</b> <b>DEFENSE-IN-DEPTH</b> Defense-in-depth provide sequential layers of protection against attacks, namely through forming zones (like onion layers) of increasing control de...	<b>ARCHITECTURE</b> <b>DEVICE-LEVEL HARDWARE AND SOFTWARE CONTROLS</b> Many devices offer low-level controls (such as protected rings) around the ...	<b>ARCHITECTURE</b> <b>ENDPOINT CONTROLS</b> Typical endpoints include desktop and mobile devices, often with standard operating systems that differ from the host / backend world. Controls inclu...	<b>ARCHITECTURE</b> <b>LOG MANAGEMENT</b> Log files are generated in various contexts across applications and operating systems. In terms of controls, log files should be manage...
<b>ARCHITECTURE</b> <b>NETWORK INFRASTRUCTURE</b> Network infrastructure controls are based on the various layers of the OSI model, ranging from physical through logical to presentation layer control ...	<b>ARCHITECTURE</b> <b>PERIMETER CONTROLS</b> Perimeter controls are designed to provide protection at the outer boundary of the enterprise, or its sphere of interest. The actual perime...	<b>ARCHITECTURE</b> <b>USER / MANAGEMENT AWARENESS</b> End users, including management, need to be aware of cybersecurity, in...	<b>DATA MANAGEMENT</b> <b>ACCESS CONTROL</b> One of the central control sets in cybersecurity is access control in the wide sense of the word. Access to information assets should be restrict...
<b>DATA MANAGEMENT</b> <b>CLASSIFICATION</b> Data and information asset classification is an important prerequisite to any cybersecurity planning, design, implementation an...	<b>DATA MANAGEMENT</b> <b>DATA INTEGRITY</b> Integrity-based controls in cybersecurity are typically applied to data at rest and data in flow (transaction controls). Technically, th...	<b>DATA MANAGEMENT</b> <b>DATA PRIVACY</b> Privacy controls in cybersecurity are an important element of defense in depth, particularly as they relate to personally identifiable information (...)	<b>DATA MANAGEMENT</b> <b>DATA RETENTION / DISPOSAL</b> Retention and archiving controls typically include secure storage of a ...

# DES PUBLICATIONS, LIVRES BLANCS ET DOCUMENTS DE RECHERCHE

Home > Publications, Whitepapers and Research

## PUBLICATIONS, WHITEPAPERS AND RESEARCH



# MANUEL DE COURS DU CSX



STUDY GUIDE



# CYBERCRIME : DÉFENDRE VOTRE ENTREPRISE

## COMMENT PROTÉGER VOTRE ORGANISATION CONTRE LES CYBERMENACES ÉMERGEANTES



### Cybercrime: Defending Your Enterprise

How to Protect Your Organization From Emerging Cyberthreats

**Abstract**

Over the last 25 years, cybercrime silently evolved from an abstract idea into a tangible threat to the global marketplace and security sector. The sharp increase of Internet-based attacks over the last five years has resulted in nation-states, enterprises, media and cyber security experts openly discussing this dire problem. Ineffective coordination of public and private entities to affect positive change toward the common goal of Internet protection across the world increasingly emboldens cybercriminals. This ineffective coordination manifests itself in a lack of incident data sharing and cooperation, and incompatible laws and regulations to mitigate nefarious activities in the digital space. Despite the infancy of global cooperation to defend against emerging global cyberthreats, an enterprise can establish measures to better protect itself. This whitepaper helps you to gain a better understanding of some of the more prominent emerging cyberthreats and arms you with measures to defend your enterprise from these threats.

# CYBERCRIME : DÉFENDRE VOTRE ENTREPRISE

## COMMENT PROTÉGER VOTRE ORGANISATION CONTRE LES CYBERMENACES ÉMERGEANTES



### The Cyberresilient Enterprise: What the Board of Directors Needs to Ask

#### Abstract

As enterprises strive to gain value by leveraging technology, the risk associated with digital business is increasing. Theft of personal information and private business information, misappropriation of resources, denial of service, and cybertheft are becoming commonplace, affecting large and small enterprises. Isolated approaches to information security, business continuity and incident response are a thing of the past; today, the urgency of providing continuously available services for customers and business partners in the digital economy requires enterprises to become resilient. A resilient enterprise protects itself from attack, but also recognizes that defense is not the end-all. A resilient enterprise needs to connect protection and recovery to the mission and goals of the enterprise, implementing integrated programs in order to provide sustainability of essential services. Board members need to evaluate the operational risk inherent in digital business and direct management to ensure that the enterprise is more than just protected—it is resilient.



# GUIDE DE MISE EN ŒUVRE DU RÉFÉRENTIEL EN CYBERSÉCURITÉ DU NIST EN UTILISANT COBIT5 (1/5)



Implementing the NIST  
Cybersecurity  
Framework



# GUIDE DE MISE EN ŒUVRE DU RÉFÉRENTIEL EN CYBERSÉCURITÉ DU NIST EN UTILISANT COBIT5 (2/5)



**Figure 1—CSF Implementation—Target Audience and Benefits**

Framework Role	Role/Function	Benefit of/Reason for Applying the Framework
Executive	Board and Executive Management	<ul style="list-style-type: none"> <li>• Understanding of their responsibilities and roles in cybersecurity within the organization</li> <li>• Better understanding of current cybersecurity posture</li> <li>• Better understanding of cybersecurity risk to the organization</li> <li>• Better understanding of cybersecurity target state</li> <li>• Understanding of actions required to close gaps between current cybersecurity posture and target state</li> </ul>
Business/Process	IT Management	<ul style="list-style-type: none"> <li>• Awareness of business impacts</li> <li>• Understanding relationship of business systems and their associated risk appetite</li> </ul>
Business/Process	IT Process Management	<ul style="list-style-type: none"> <li>• Understanding of business requirements and mission objectives and their priorities</li> </ul>
Business/Process	Risk Management	<ul style="list-style-type: none"> <li>• Enhanced view of the operational environment to discern the likelihood of a cybersecurity event</li> </ul>
Business/Process	Legal Experts	<ul style="list-style-type: none"> <li>• Understanding of cyberthreats to the business units and their mission objectives</li> <li>• Understanding of all compliance requirements for each business unit</li> </ul>
Implementation/Operator	Implementation Team	<ul style="list-style-type: none"> <li>• Understanding of security controls and their importance in managing operational security risk</li> <li>• Detailed understanding of required actions to close gaps in cybersecurity requirements</li> </ul>
Implementation/Operator	Employees	<ul style="list-style-type: none"> <li>• Understanding of cybersecurity requirements for their associated business systems</li> </ul>

# GUIDE DE MISE EN ŒUVRE DU RÉFÉRENTIEL EN CYBERSÉCURITÉ DU NIST EN UTILISANT COBIT5 (3/5)



Figure 8—Comparison of CSF Implementation Steps With COBIT 5 Principles

CSF Implementation Steps	COBIT 5 Principles
<p><b>Step 1: Prioritize and Scope</b>—Directs implementers to identify business/mission objectives and high-level organizational priorities. This mission understanding is critical to ensure that resulting risk decisions are prioritized and aligned with stakeholder goals, ensuring effective risk management and optimizing investment.</p>	<p><b>Principle 1: Meeting Stakeholder Needs</b>—Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources. An enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific goals and map these to specific processes and practices.</p>

# GUIDE DE MISE EN ŒUVRE DU RÉFÉRENTIEL EN CYBERSÉCURITÉ DU NIST EN UTILISANT COBIT5 (4/5)



Figure 12—Framework Core Identifiers and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Information
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, USA, 2014, Table 1

# GUIDE DE MISE EN ŒUVRE DU RÉFÉRENTIEL EN CYBERSÉCURITÉ DU NIST EN UTILISANT COBIT5 (5/5)



**CSF Step 1: Prioritize and Scope.**  
COBIT Phase 1—What Are the Drivers?

**CSF Step 2: Orient, and Step 3: Create a Current Profile**  
COBIT Phase 2—Where Are We Now?

**CSF Step 4: Conduct a Risk Assessment, and Step 5: Create a Target Profile**  
COBIT Phase 3—Where Do We Want To Be?

**CSF Step 6: Determine, Analyze, and Prioritize Gaps.**  
COBIT Phase 4—What Needs To Be Done?



**CSF Step 7: Implement Action Plan**  
COBIT Phase 5—How Do We Get There?

**CSF Action Plan Review**  
COBIT Phase 6—Did We Get There?

**CSF Life Cycle Management**  
COBIT Phase 7—How Do We Keep the Momentum Going?



# AUDITER LA CYBERSÉCURITÉ: ÉVALUER LES RISQUES ET AUDITER LES CONTRÔLES



## ABSTRACT

Cyber security has become a prevalent issue today facing most organizations, one that is recognized by companies to be an enterprisewide issue requiring thoughtful attention. Investments in controls are necessary to protect organizations from increasingly sophisticated and widely available attack methods. Intentional attacks, breaches and incidents can have damaging consequences. This white paper highlights the need for these controls implemented as part of an overall framework and strategy, and focuses on the subsequent assurance that is needed through management review, risk assessments and audits of the cyber security controls.



## IS AUDIT/ASSURANCE PROGRAM Cybersecurity: Based on the NIST Cybersecurity Framework



# UN FORUM DE DISCUSSION

**Featured Topics** | Browse Over 100 Topics | Search Topics | My Topics

Find Resources & Connect with members on topics that interest you.

Young Professionals | Business Continuity-Disaster Recovery Planning | COBIT - Use It Effectively | Mobile Computing | SUGGEST A NEW TOPIC

Oracle Database | Strategic Planning/Alignment



### CyberSecurity



Share knowledge about CyberSecurity with other ISACA members and identify and discuss issues that need more guidance from ISACA. Collaborate, make connections and learn how to keep your organization safe from Cyber risks.

LEAVE THIS COMMUNITY




ISACA members can participate by clicking on the "Join this Community" button. You must be signed into the site. Set your alerts to be notified of new discussion activity within this community. Not an ISACA member? Join now!

#### Community Leader




 **Claudio Cilli**  
Badge: 

 **M.Lambert**  
Title: CISO  
Badge: 

#### This Topic Has:

 3216 Members  
 5 Online  
 24336 Visits


#### Recent Discussions


-  The economics of cyber is going in the wrong direction. Posted by Ron Hale Ph.D. CISM.
-  Montreal researcher helped convict one of gang behind Li... Posted by M.Lambert.
-  Last Chance to Help Shape NIST's Updated Cyber Framework. Posted by M.Lambert.

[View All »](#)


#### NEW! Activity Badges

Badges help others understand your level of community activity and your reputation as a contributor within the Knowledge Center. [Learn More.](#)











**Discussions:** 500 total 

**START A DISCUSSION** | [View All »](#)

 **The economics of cyber is going in the wrong direction**  
Before we can hope to address current cyber problems we need to solve legacy issues. Spam continues to grow but it gets very little public attention. <http://csoonline.com/article/3185465/internet/the-economics-of-cyber-is-going-in-the-wrong-direction.htm...>  
Ron Hale Ph.D. CISM | 4/7/2017 2:33:17 PM | COMMENTS(0)

#### Newest Members (10)

-  **Austin742**  

-  **proferyk**  
Cyber Security Consultant  

-  **Stanley990**  
IT Security Manager  

-  **Yusup Ardhan**  


# SANS OUBLIER LE SITE D'ISACA-QUÉBEC:

## Nouvelles en continue

### 2017-04-11 - On sait ce qu'est la cyberguerre, mais comment construire la cyberpaix ?

Quelle sont les conditions d'une cyberpaix ? Que faut-il mettre en place pour garantir au maximum un espace numérique bienveillant ? C'est la question qui a [...]

### 2017-04-11 - Piratage des élections américaines : un Russe arrêté et incarcéré en Espagne

Piotr Levachov est soupçonné d'avoir participé à des cyberattaques menées durant la campagne électorale américaine. [...]

### 2017-04-11 - Les fausses promesses de la cybersécurité

Ne croyez pas aux promesses de la cybersécurité pour vous protéger. Des hackers ont ainsi volé 81 millions [...]

▶ [LIRE TOUTES LES NOUVELLES](#)

### Les activités proposées par l'ISACA Québec

- Journées conférence en lien avec les thèmes de l'association
- Formations données par des professionnels
- Activités de réseautage pour réunir les membres de l'ISACA Québec

 [TÉLÉCHARGER PROGRAMMATION .PDF](#)



# MERCI



David Henrard, CISA, CISM, CRISC  
Responsable de la pratique “Sécurité”  
[david.henrard@levio.ca](mailto:david.henrard@levio.ca)

