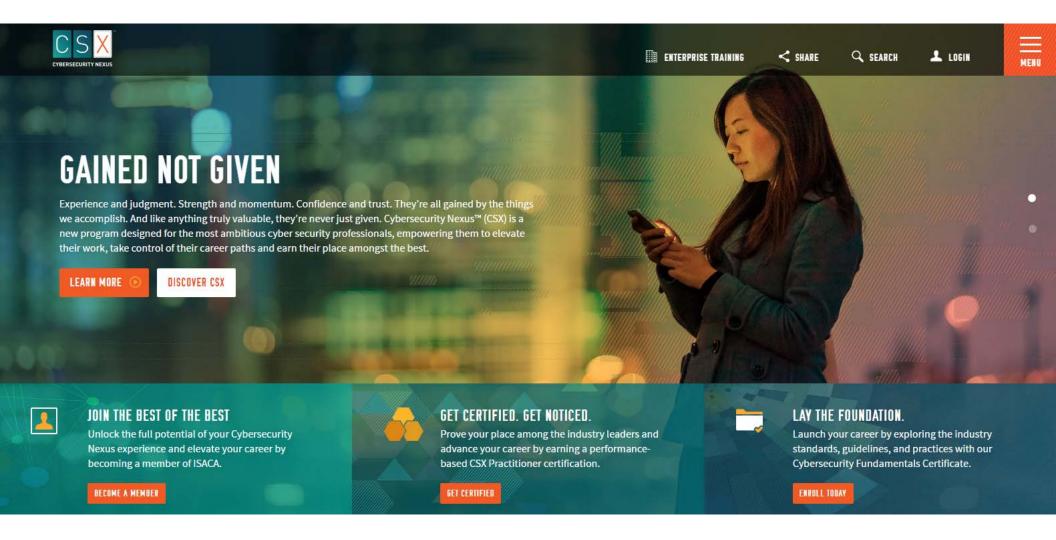


# ISACA, UNE SOURCE D'INFORMATION INCONTOURNABLE EN CYBERSÉCURITÉ

DAVID HENRARD, CISA, CISM, CRISC



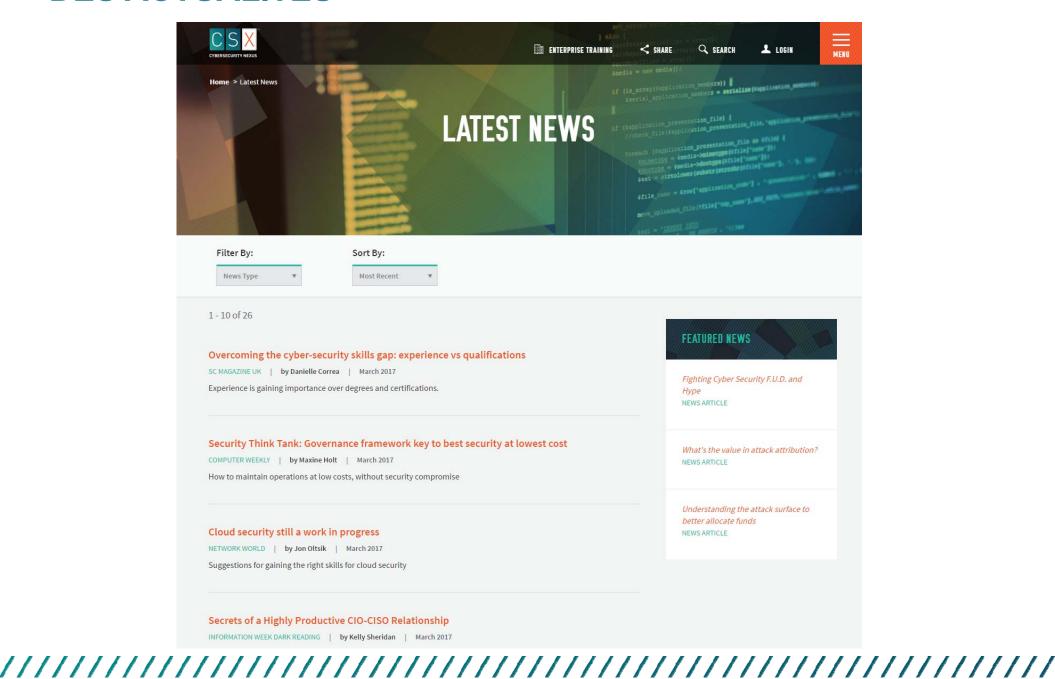
## LA PLATEFORME CSX HTTPS://CYBERSECURITY.ISACA.ORG/







### **DES ACTUALITÉS**







### 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.



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

03:10 PM EST

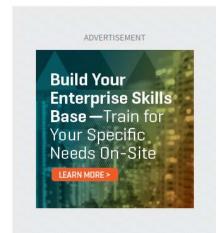
A previously undisclosed baseband vulnerability impacting Huawei smartphones, laptop WWAN modules and IoT components was revealed Thursday at the Infiltrate Conference



#### 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 pentesting and raised \$15,000 for charity in the process.







#### **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.







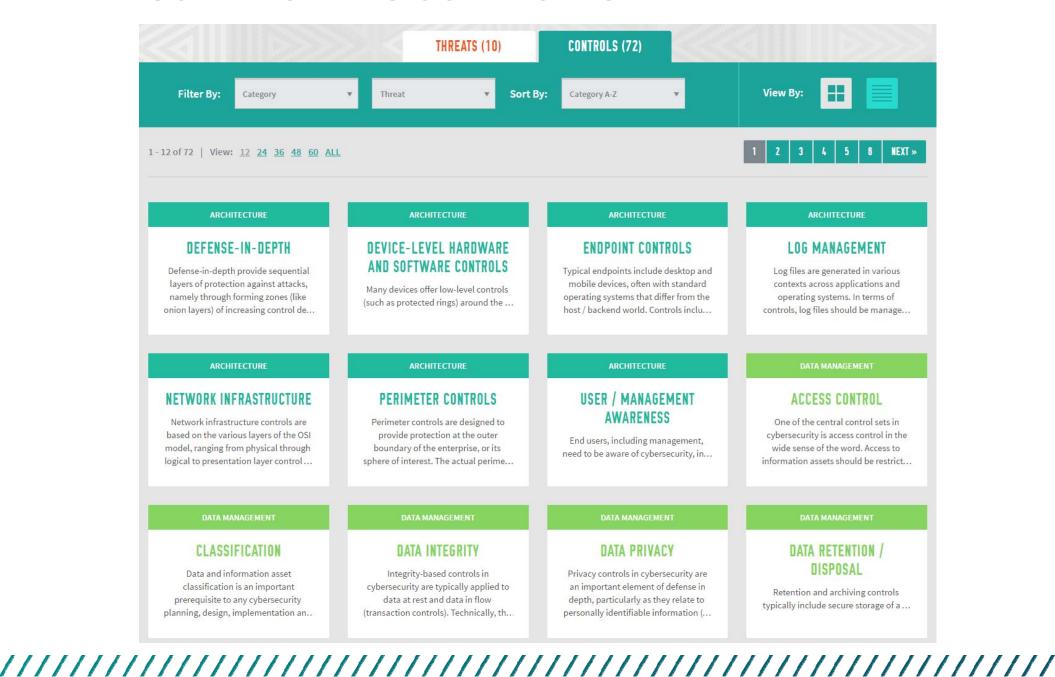
### LA DESCRIPTION DES MENACES

THREATS (10) CONTROLS (72) View By: Sort By: A-Z CYBERCRIME INSIDER THREATS APT DDOS Advanced Persistent Threats (Generic) Cybercrime (Generic) The term Distributed Denial of Service (Generic) Insider Threat (Generic) An insider "cybercrime" includes a wide range of The term "denial of service" generally threat is defined as the potential of an The term "advanced persistent threat" (APT) denotes a type of threat and criminal acts directed at individuals or denotes an attack, or series of attacks, adverse act or omission from within attack that is technically sophisticated enterprises. The specific background on an IT environment, with a view to the organization, i.e., committed by and usually present in the context of... to calling a criminal act a "cybercrim... disrupting or disabling the services p... employees or individuals with a spec... SOCIAL ENGINEERING MALWARE MOBILE MALWARE RANSOMWARE Malware (Generic) The term Mobile Malware (Generic) Mobile Ransomware (Generic) The term Social Engineering (Generic) The term "malware" denotes any malicious malware denotes a specific type of "ransomware" denotes the insertion "social engineering" incorporates any software used for the purpose of malware that affects mobile devices, of malware that is designed to extort a and all human-intelligent interactions attacking systems and IT most notably smartphones. The ransom in money or money equivalent that are designed to elicit an environments. There is a vast numbe... emergence of mobile malware has b... from the end user. This is usually ach... involuntary or unconscious response... WATERING HOLE **UNPATCHED SYSTEMS** Unpatched Systems (Generic) Watering Hole (Generic) The term Unpatched systems are programs for "watering hole" denotes a technique which a patch-software that modifies whereby end users visiting a certain a system, application or other web site are covertly redirected to program-is either unavailable or ha... another web site that will deliver ma...





### LA DESCRIPTION DES CONTRÔLES







## DES PUBLICATIONS, LIVRES BLANCS ET DOCUMENTS DE RECHERCHE

PUBLICATIONS, WHITEPAPERS AND RESEARCH

PUBLICATIONS, WHITEPAPERS AND RESEARCH

(\*Application\_presents)





### MANUEL DE COURS DU CSX











### CYBERCRIME: DÉFENDRE VOTRE ENTREPRISE

COMMENT PROTÉGER VOTRE ORGANISATION CONTRE LES CYBERMENACES ÉMERGEANTES





## Cybercrime: Defending Your Enterprise

How to Protect Your Organization From Emerging Cyberthreats







### CYBERCRIME : DÉFENDRE VOTRE ENTREPRISE

COMMENT PROTÉGER VOTRE ORGANISATION CONTRE LES CYBERMENACES ÉMERGEANTES





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







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











# 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> <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	Awareness of business impacts     Understanding relationship of business systems and their associated risk appetite		
Business/Process	IT Process Management	Understanding of business requirements and mission objectives and their priorities		
Business/Process	Risk Management	Enhanced view of the operational environment to discern the likelihood of a cybersecurity event		
Business/Process Legal Experts		<ul> <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	Understanding of security controls and their importance in managing operational security risk     Detailed understanding of required actions to close gaps in cybersecurity requirements		
Implementation/ Operator	Employees	Understanding of cybersecurity requirements for their associated business systems		





# 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		
Step 1: Prioritize and Scope—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.	Principle 1: Meeting Stakeholder Needs— 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.		





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



Figure 12—Framework Core Identific	ers and Categories
------------------------------------	--------------------

Function Unique Identifier	Function	Category Unique Identifier	Category
		AM	Asset Management
		BE	Business Environment
ID	Identify	GV	Governance
		RA	Risk Assessment
		RM	Risk Management
<b>PR</b> Pro		AC	Access Control
		AT	Awareness and Training
	Protect	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



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. Cybersecurity:
Based on the NIST
Cybersecurity
Framework

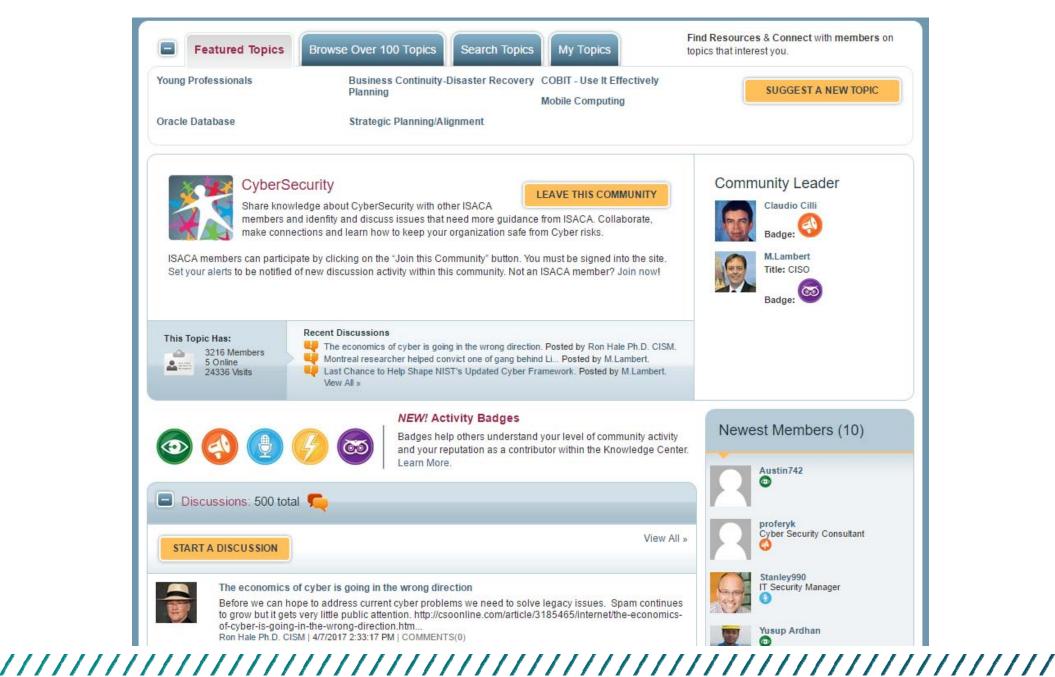








#### **UN FORUM DE DISCUSSION**







### SANS OUBLIER LE SITE D'ISACA-QUÉBEC:





LE CHAPITRE

ACTIVITÉS

CERTIFICATIONS

**PUBLICATIONS** 

**PARTENARIATS** 

**EMPLOIS** 

#### 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 [...]

 $\blacktriangleright$ 

LIRE TOUTES LES NOUVELLES

Les activités proposées par l'ISACA Québec

- Journées conférence en lien avec
- 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

