



โครงการเสวนาคลินิกไอเอครั้งที่ 8/2559

"Readiness against Cyber Risk"

ผู้ดำเนินการเสวนา

- **คุณสมชัย แพทย์วิบูลย์**
Senior IT Auditor
ธนาคารไอซีบีซี (ไทย) จำกัด(มหาชน)
- **คุณเสนีย์ วัชรศิริธรรม CISA, CGEIT, CRISC**
ผู้อำนวยการตรวจสอบเทคโนโลยีสารสนเทศ
ธนาคารไทยพาณิชย์

ISACA

- สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ ภาคพื้นกรุงเทพฯ
2 อาคารมูลนิธิคีนันต์คาเบรียลแห่งประเทศไทย ซอยทองหล่อ 25 สุขุมวิท 55 เขตวัฒนา กทม.
10110
โทรศัพท์: 089-777-0900
- member@isaca-bangkok.org
- <http://www.isaca-bangkok.org>
-  : ISACA.BKK
-  : @isaca-bangkok
-  : isacabangkok

<http://www.isaca.org/CERTIFICATION/Pages/default.aspx>

			
What is CISA	What is CISM	What is CGEIT	What is CRISC
Benefits of CISA	Benefits of CISM	Benefits of CGEIT	Benefits of CRISC
How to Become Certified	How to Become Certified	How to Become Certified	How to Become Certified
June 2015 Exam Information	June 2015 Exam Information	June 2015 Exam Information	June 2015 Exam Information
Apply for Certification	Apply for Certification	Apply for Certification	Apply for Certification
Maintain Your CISA	Maintain Your CISM	Maintain Your CGEIT	Maintain Your CRISC
▶ Why Certify	▶ Maintain Your Certification	▶ Write an Exam Question	▶ US DoD Information
▶ How to Earn CPE			▶ Exam Registration

Key Exam Registration Dates:

13 June 2015 Exam

3 November 2014
13 February 2015
10 April 2015

Registration Opens
Early Registration Deadline
Final Registration Deadline

[REGISTER FOR THE JUNE EXAM](#)

Cyber security NEXUS

ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE CENTER JOURNAL BOOKSTORE

ISACA > cyber

CSX™
CYBERSECURITY NEXUS

Insights and resources for the cybersecurity professional from ISACA

CYBERSECURITY NEXUS

Visit Cybersecurity Legislation Watch and Read our New CSX SPECIAL REPORT! [READ REPORT >>](#)

OVERVIEW

In enterprise IT, there is a single point where everything that matters in information, technology and business converges: Cybersecurity Nexus (CSX), a new security knowledge platform and professional program from ISACA.

CSX is helping shape the future of cybersecurity through cutting-edge thought leadership, as well as training and certification programs for the professionals who are leading it there. Building on the strength of ISACA's globally-recognized expertise, it gives cybersecurity professionals a smarter way to keep organizations and their information more secure.

With CSX, business leaders and cyber professionals can obtain the knowledge, tools, guidance and connections to be at the forefront of a vital and rapidly changing industry. Because Cybersecurity Nexus is at the center of everything that's coming next.

CREDENTIALING

Secure recognition for your expertise. Our globally accepted certifications help advance skills and careers.

- > CYBERSECURITY FUNDAMENTALS CERTIFICATE NOW AVAILABLE
- > CISM
- > SIGN UP to receive information about upcoming CSX certifications.

MEMBERSHIP

Join a global community of more than 115,000 professionals, innovators and thought leaders.

- > PROFESSIONAL MEMBERSHIP
- > STUDENT MEMBERSHIP

WHAT'S NEW

Experience With the Framework for Improving Critical Infrastructure Cybersecurity (ISACA responded to the NIST request for comments on experience with the Framework for Improving Critical Infrastructure Cybersecurity).

Advanced Persistent Threat Awareness Study Results: Only 15% of enterprises say they're very prepared for APTs, and 1 in 5 have already been attacked.

Cybersecurity Fundamentals Certificate Exam: ISACA's first-ever certificate focused on the concepts that frame and define the growing and rapidly changing field of cybersecurity.

CYBERSECURITY NEXUS NEWSROOM

EDUCATION / CONFERENCES

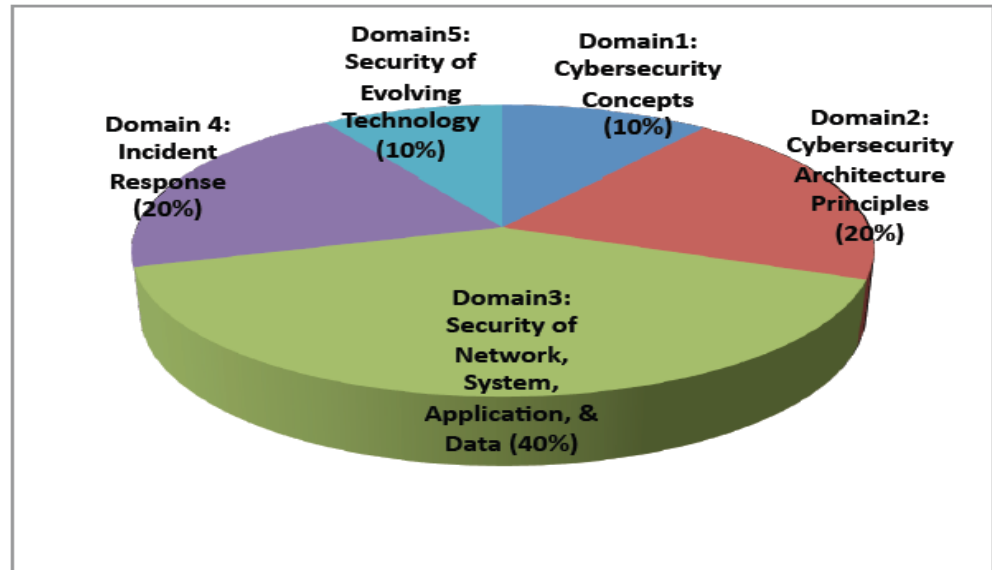
Enhance your cybersecurity knowledge and skills at our global conferences, workshops and training events.

- > CONFERENCES
 - Euro CACS / ISRM + Cyberlympics World Finals
 - North America ISRM
 - Latin CACS / ISRM
- > WEBINARS
- > VIRTUAL CONFERENCES
- > WORKSHOPS
 - Cybersecurity Fundamentals Workshop - Euro CACS/ISRM

RESOURCES / PUBLICATIONS

Find the latest research and expert thinking on standards, best practices, emerging trends and beyond.

- > ARTICLES FROM ISACA JOURNAL
- > CYBERSECURITY BLOG POSTS
- > WHITE PAPERS & PUBLICATIONS
 - European Cybersecurity Implementation Series
 - Cybersecurity Fundamentals Study Guide™
 - Cybersecurity: What the Board of Directors Needs to Ask
 - IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK
 - RESPONDING TO TARGETED CYBERATTACKS™
- > TRANSFORMING CYBERSECURITY™



Remove	Item #	Type	Description	Qty	Unit Price	Ext. Price
<input type="checkbox"/>	CSX_FUNDCERT	SALES	Cybersecurity Fundamentals Certificate	1	\$150.00	\$150.00
<input type="checkbox"/>	CSXG1	SALES	CSX Cybersecurity Fundamentals Study Guide	1	\$45.00	\$45.00
<input type="checkbox"/>	CSXS	SALES	Cybersecurity Fundamentals Print Bundle	1	\$0.00	\$0.00
<input type="checkbox"/>	RDMP_CSX	SALES	Cybersecurity Fundamentals Exam and Study Guide Bundle	1	(\$10.00)	(\$10.00)
Subtotal:						\$185.00
Shipping(FEDEX):						\$15.00
Total before tax:						\$200.00
Estimated tax:						\$0.00
Order Total:						\$200.00
<input type="button" value="Clear cart"/>	<input type="button" value="Update cart"/>	<input type="button" value="Print"/>	<input type="button" value="Enter Code"/>	<input type="button" value="Pay by Check or Bank Transfer"/>	<input type="button" value="Checkout - Pay by Credit Card"/>	

http://www.isaca-bangkok.org

ISACA
Bangkok Chapter

Home
Welcome to ISACA Bangkok Chapter
IA Client_8_2668

เว็บไซต์นี้จัดทำและดูแลโดย บริษัท ไอ.เอส.เอ.ซี. จำกัด

เชิญผู้สนใจเข้าร่วมงานเสวนาออนไลน์ ครั้งที่ 8/2559
สมาคมผู้ตรวจการสอบภายในแห่งประเทศไทย, สถาบันผู้ตรวจการสอบภายใน
ร่วมกับ
ISACA Bangkok Chapter และ ISSMF Thailand Association
จัดเสวนาวิชาการเกี่ยวกับ
"Readiness against Cyber Risk"

โดยจัดขึ้นในวันอาทิตย์ที่ 20 สิงหาคม 2559 เวลา 9.00 - 12.00 น.
สถานที่ ชั้น 5 อาคาร 501-502 ชั้น 5 อาคารผู้พิทักษ์ประเทศไทย
ถ.วิภาวดีรังสิต ชั้น 501-502 ชั้น 5 อาคารผู้พิทักษ์ประเทศไทย ร.พ.วิภาวดี 30

ผู้ดำเนินการเสวนา
คุณสมศักดิ์ วิชาญใจธรรม OSA, CGEIT, CRISC ผู้ดำเนินการตรวจประเมินเทคโนโลยี
สารสนเทศ ธนาคารไทยพาณิชย์

ผู้จัดเสวนา
คุณสมศักดิ์ แหม่มวิบูลย์ Senior IT Auditor ธนาคารไทยพาณิชย์ (MFI-บริษัท) ธนาคาร
กรุงศรีอยุธยา

ITAE
Val IT
Risk IT

Feed Entries

Who's Online
Advertisement
Related Links

COBIT 5

- COBIT 5 Framework
- COBIT 5 Implementation
- COBIT 5: Enabling Processes
- COBIT 5: Enabling Information
- COBIT 5 for Information Security
- COBIT 5 for Assurance
- COBIT 5 for Risk
- Process Assessment Model
- Self-Assessment Guide
- Assessor Guide

http://www.isaca.org/COBIT/Pages/COBIT-5-Thai.aspx

ISACA
Trust in, and value from, information systems

Support Shopping Cart Join ISACA Sign In **ENGLISH**

ISACA My ISACA Site Content SEARCH Advanced Search

ABOUT MEMBERSHIP CERTIFICATION EDUCATION COBIT KNOWLEDGE CENTER JOURNAL BOOKSTORE

CSX CYBERSECURITY NEXUS Insights and resources for the cybersecurity professional from ISACA. [Learn More](#)

ISACA > COBIT > COBIT 5 Thai share

COBIT 5 Thai


COBIT 5 Thai
 Download: Member | Non-Member (complimentary)
 Purchase in Book Format: Member US \$35 | Non-Member US \$40

COBIT 5 Enabling Processes ภาษาไทย (Thai)
 Download: Member (complimentary) | Non-Member US \$50
 Purchase in Book Format: Member US \$35 | Non-Member US \$55


COBIT 5 Implementation ภาษาไทย (Thai)
 Download: Member (complimentary) | Non-Member US \$50

ผลิตภัณฑ์นี้สามารถสั่งซื้อได้ในรูปแบบสิ่งพิมพ์ ด้วยจำนวนต่ำสุด 20 เล่ม

[Return to Product Family page](#)



ISACA
COBIT
5
กรอบการดำเนินงานของธุรกิจสำหรับ
การกำกับดูแลและการบริหารการ
ไอทีระดับโลก



COBIT
6

Topic

ช่วงที่ 1

- แนะนำสมาคมฯ
- ภาพรวม **Cyber Security , Cyber Risk**
- **Five Key Cybersecurity Trends for 2016**
- **January 2016 Cybersecurity Snapshot Global Results**

ช่วงที่ 2

- เสวนา ถามตอบปัญหา

Effective January 1, 2013

มาตรฐานสากลการปฏิบัติงานวิชาชีพการตรวจสอบภายใน

**INTERNATIONAL STANDARDS
FOR THE PROFESSIONAL PRACTICE
OF INTERNAL AUDITING**

1210-ความเชี่ยวชาญเชิงวิชาชีพ

1210.A3

ผู้ตรวจสอบภายในต้องมีคามรู้เพียงพอเกี่ยวกับความเสี่ยงและการควบคุมหลักของเทคโนโลยี

9

ผู้ตรวจสอบภายในทุกคนไม่จำเป็นต้องมีความเชี่ยวชาญเทียบเท่ากับผู้ตรวจสอบภายในที่รับผิดชอบงานตรวจสอบเทคโนโลยีสารสนเทศโดยตรง

1220-ความระมัดระวังเยี่ยงวิชาชีพ

1220.A2 - ในการปฏิบัติหน้าที่ด้วยความระมัดระวังเยี่ยงวิชาชีพ
ผู้ตรวจสอบภายในต้องพิจารณาใช้เทคนิคการตรวจสอบด้วยเทคโนโลยีและเทคนิคการวิเคราะห์
ข้อมูลอื่นๆ เป็นเครื่องมือช่วยในงานตรวจสอบ

2210-วัตถุประสงค์ของภารกิจ

2110.A2

กิจกรรมการตรวจสอบภายในต้องประเมินว่าการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กรสนับสนุนวัตถุประสงค์และกลยุทธ์ขององค์กรได้หรือไม่

เทคนิคการตรวจสอบโดยใช้เทคโนโลยี - Technology-based Audit Techniques :

เครื่องมือหรือโปรแกรมคอมพิวเตอร์ช่วยตรวจสอบประเภทต่างๆ เช่น

โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบแบบทั่วไป (Generalized Audit Software),

โปรแกรมคอมพิวเตอร์ที่ช่วยสร้างข้อมูลเพื่อใช้ตรวจสอบ (Test data generators),

โปรแกรมการตรวจสอบแบบ computerized, โปรแกรมคอมพิวเตอร์ช่วยตรวจสอบแบบเฉพาะทาง

(Specialized audit utilities) และ CAATs (Computer Assisted Audit Techniques)

การควบคุมด้านเทคโนโลยีสารสนเทศ – Information Technology Controls :

การควบคุมที่สนับสนุนการบริหารจัดการและการกำกับดูแลธุรกิจ โดยจัดให้มีการควบคุมที่โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ เช่น ระบบงาน ข้อมูล ระบบโครงสร้าง และบุคลากร

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ – Information Technology Governance :

ประกอบด้วยภาวะความเป็นผู้นำ โครงสร้างขององค์กร และกระบวนการที่สร้างความมั่นใจว่า เทคโนโลยีสารสนเทศขององค์กรสนับสนุนกลยุทธ์และวัตถุประสงค์ขององค์กร

<https://www.techtalkthai.com/category/security/>

รัสเซียเผย Critical Infrastructure กำลังถูกมัลแวร์โจมตี

techtalkthai August 4, 2016 Security, Threats Update



Federal Security Service (FSB) ของรัสเซียออกมาเปิดเผยว่า ระบบเครือข่ายทางการทหารและระบบโครงสร้างพื้นฐานสำคัญหลายระบบของรัสเซีย กำลังตกเป็นเป้าหมายโจมตีของมัลแวร์ตัวฉกาจ ซึ่งจ้องจารกรรมข้อมูลสำคัญของรัฐบาลสู่ภายนอก

[Read More »](#)

 Like 136

 Tweet

 G+ 1

 Share 1

<https://www.techtalkthai.com/category/security/>

ระบบ IT ของสายการบิน DELTA ไฟดับ ส่งผลให้เที่ยวบิน DELTA ทั่วโลก ต้องดีเลย์หรือยกเลิก

🕒 August 8, 2016 📁 IT Case Studies, IT Knowledge

สายการบิน Delta ได้ออกมาแถลงถึงสาเหตุของการที่เที่ยวบินทั้งหมดของ Delta ทั่วโลกต้องดีเลย์ด้วยสาเหตุอันเนื่องมาจากเหตุไฟดับที่ Atlanta ทำให้ระบบคอมพิวเตอร์และกระบวนการทำงานต่างๆ ของ Delta ทั่วโลกต้องหยุดชะงักลง

<https://www.techtalkthai.com/category/security/>

Ransomware รูปแบบใหม่ ฟุ่งเป้าระบบควบคุมอุณหภูมิอัจฉริยะ

techtalkthai © August 9, 2016

Cloud and Systems, Endpoint Security, Internet of Things, Internet of Things Security, IT Knowledge, IT Seminars and Training, Security, Threats Update



จ่ายค่าไถ่ซะ ถ้าไม่อยากร้อน !! Ken Munro และ Andrew Tierney นักวิจัยจาก Pen Test Partners บริษัทให้คำปรึกษาด้านความมั่นคงปลอดภัยชื่อดังจากสหราชอาณาจักร ได้สาธิต Ransomware รูปแบบใหม่โดยมีเป้าหมายที่ระบบควบคุมอุณหภูมิอัจฉริยะ ซึ่งช่วยให้แฮ็คเกอร์สามารถล็อกอุณหภูมิได้ตามความต้องการ เหยื่อจำเป็นต้องจ่ายค่าไถ่ถ้าไม่อยากให้บ้านของตนร้อน

[Read More »](#)

 Like 132

 Tweet

 G+ 1

 Share 1



<https://www.techtalkthai.com/category/security/>

พบ SAP กว่า 36,000 ระบบเชื่อมต่อออนไลน์ เสี่ยงตกเป็นเป้าหมายของการโจมตี

techtalkthai August 2, 2016

Applications, Cloud and Systems, Cloud Security, Cloud Services, Endpoint Security, IT Knowledge, IT Trends and Updates, Mobile Enterprise, Mobile Security, Products, SAP, Security, Threats Update, Web Security



ERPScan ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบ ERP ออกรายงาน SAP Cybersecurity Threat Report ฉบับล่าสุด แบ่งเป็น 3 หัวข้อหลัก คือ Product Security, Implementation Security และ Security Awareness ระบบ พบ SAP กว่า 36,000 ระบบเชื่อมต่อกับอินเทอร์เน็ต ทั้งๆ ที่ควรเป็นระบบปิด เปิดช่องให้แฮ็คเกอร์สามารถโจมตีได้

[Read More »](#)

<https://www.techtalkthai.com/category/security/>

นักวิจัยพบวิธีซ่อนมัลแวร์ไว้ในไฟล์ที่ถูกเซ็นด้วย DIGITAL SIGNATURE

🕒 August 8, 2016

📁 Endpoint Security, Featured Posts, IT Knowledge, IT Seminars and Training, Physical Security, Security, Threats Update

Tom Nipravsky นักวิจัยด้านความมั่นคงปลอดภัยจาก Deep Instinct ค้นพบเทคนิคการซ่อนพรางมัลแวร์ไว้ในไฟล์ข้อมูลปกติที่ถูกเซ็นด้วย Digital Signature ซึ่งช่วยให้แฮ็คเกอร์สามารถลอบส่งมัลแวร์เข้ามาในระบบโดยที่ Antivirus ไม่สามารถตรวจจับได้ที่น่าสนใจคือ Signature ยังมีค่าเท่าเดิมไม่เปลี่ยนแปลงใดๆ ที่ข้อมูลถูกแก้ไข

<https://www.techtalkthai.com/category/security/>

Hacker 2 คนถูกจับ หลัง Hack และขโมยรถไปได้มากกว่า 30 คันด้วย Laptop เพียงเครื่องเดียว

techtalkthai August 6, 2016 Cloud and Systems, Internet of Things, Internet of Things Security, Security



ณ Houston รัฐ Texas ประเทศสหรัฐอเมริกา ได้มีการเข้าจับกุม Michael Arcee และ Jesse Zelay สอง Hacker ที่ทำการขโมยรถ Jeep และ Dodge ไปแล้วมากกว่า 30 คันโดยการใช้ Laptop เชื่อมต่อเข้ากับระบบ Software ของตัวรถ และทำการโจมตีเพื่อ Start รถและขโมยรถเหล่านั้นไป

[Read More »](#)

<https://www.techtalkthai.com/category/security/>

สู้ Hacker ด้วย Machine Learning! หาช่องโหว่ Zero Day ที่ขายใน Darknet และ Deepnet ก่อนถูกนำมาใช้โจมตีอย่างแพร่หลาย

techtalkthai August 8, 2016

Advanced Threat Protection, Big Data and Data Science, Cloud and Systems, IT Knowledge, IT Researches, Security



ทีมนักวิจัยจาก Arizona State University ได้นำเสนอแนวทางการลดความเสี่ยงจากการถูกโจมตีแบบ Zero Day ด้วยการใช้ Machine Learning (ML) เข้าไปเรียนรู้ตาม Forum และแหล่งประกาศขายช่องโหว่ Zero Day บน Darknet และ Deepnet โดยอัตโนมัติ ทำให้เหล่าผู้รักษาความปลอดภัยสามารถทราบแนวโน้มของช่องโหว่และการโจมตีต่างๆ ได้ล่วงหน้าก่อนที่การโจมตีเหล่านั้นจะถูกนำมาใช้แพร่หลาย และสามารถโต้ตอบได้อย่างรวดเร็วที่สุดเท่าที่จะเป็นไปได้

[Read More »](#)



<https://www.techtalkthai.com/category/security/>

รัฐบาลอิหร่านสั่งแบน Pokémon Go ด้วยเหตุผลทางด้านความปลอดภัย

เด็กฝึกงาน TechTalkThai หมายเลข 1 © August 6, 2016 Mobile Security, Security



หลังจากที่หลายประเทศได้ออกมาแสดงความกังวลทางด้านความปลอดภัยในการเล่นเกมน Pokémon Go ของประชาชน แต่อิหร่านกลับเป็นประเทศแรกที่สั่งแบน Pokémon Go อย่างเป็นทางการ ด้วยเหตุผลทางด้านความปลอดภัย

[Read More »](#)

<https://www.techtalkthai.com/category/security/>

Microsoft เพิ่มรางวัล Bug Bounty ให้ Edge และออกตัวแปลง Chrome Extension ให้มาใช้งาน Edge ได้

techtalkthai August 6, 2016 Microsoft, Products, Security



Microsoft ได้ประกาศเปิดรางวัล Bug Bounty สำหรับช่องโหว่ Remote Code Execution บน Microsoft Edge ใน Windows Insider Preview Build และ Open Source อย่าง Chakra ตั้งแต่ 500 - 15,000 เหรียญหรือราวๆ 17,500 - 525,000 บาท เพื่อผลักดันให้ Microsoft Edge มีความปลอดภัยมากยิ่งขึ้นกว่าเดิม ส่วนถ้าใครพบช่องโหว่ที่ทาง Microsoft พบเป็นการภายในเองอยู่ก่อนแล้ว ก็จะได้รับเงินรางวัลถึง 1,500 เหรียญหรือราวๆ 52,500 บาทเลยทีเดียว

[Read More »](#)

<https://www.techtalkthai.com/category/security/>

บัตร ATM แบบ Chip-and-pin ไม่ได้ปลอดภัยเสมอไป Rapid 7 สาธิตการแฮ็คโชว์

techtalkthai August 6, 2016 IT Knowledge, IT Seminars and Training, Products, Rapid7, Security, Threats Update



ภายในงาน Black Hat USA 2016 ที่เพิ่งจัดไปที่ลาสเวกัส ทีมนักวิจัยจาก Rapid 7 สาธิตวิธีปรับแต่งอุปกรณ์แบบง่ายๆ ซึ่งเพียงพอที่จะให้แฮ็คเกอร์สามารถบายพาสระบบป้องกัน Chip-and-Pin ของบัตร ATM เพื่อขโมยเงินจากตู้ ATM หรือทำธุรกรรมโดยไม่ได้รับอนุญาตได้

[Read More »](#)

 Like 467

 Tweet

 1

 Share 2



<https://www.techtalkthai.com/category/security/>

Cerber2 Ransomware เวอร์ชันใหม่ ยังไม่มีวิธีปลดล็อก

techtalkthai © August 9, 2016 Endpoint Security, Products, Security, Threats Update, Trend Micro



หลังจากที่ Trend Micro ผู้ให้บริการโซลูชันด้านความมั่นคงปลอดภัย ออก Decrypter สำหรับปลดล็อกไฟล์ข้อมูลที่ถูกเข้ารหัสด้วย Ransomware ชื่อดังหลายรายการเมื่อไม่กี่สัปดาห์ที่ผ่านมา ไม่ว่าจะเป็น Cerber, CryptXXX, BadBlock และ TeslaCrypt พบว่าแฮ็คเกอร์ ได้ลอบดูโค้ดและทำการอัปเดต Cerber Ransomware เป็นเวอร์ชันใหม่ Cerber2 ซึ่งยังไม่สามารถปลดรหัสได้นอกจากจะจ่ายค่าไถ่

[Read More »](#)



<https://www.techtalkthai.com/category/security/>

Petya และ Mischa พร้อมให้บริการ Ransomware-as-a-Service

techtalkthai July 27, 2016 Endpoint Security, Security, Threats Update



ทีมแฮ็คเกอร์ Petya และ Mischa Ransomware เปิดโอกาสธุรกิจมืด
แนวใหม่ พร้อมให้เหล่าแฮ็คเกอร์ทั้งมือสมัครเล่นและมีอาชีพเป็น
ตัวแทนกระจาย Ransomware ชื่อดังผ่านบริการ Ransomware-as-a-
Service ซึ่งค่าไถ่ที่ได้จะถูกแบ่งให้ทางทีมแฮ็คเกอร์และตัวแทน
กระจายตามอัตราส่วนที่ตกลงกันไว้

[Read More »](#)

 Like 145

 Tweet

 G+ 2

 Share 1

<https://press.malwarebytes.com/2016/08/03/international-study-finds-nearly-40-percent-of-enterprises-hit-by-ransomware-in-the-last-year/>



International Study Finds Nearly 40 Percent of Enterprises Hit By Ransomware in the Last Year

Crippling threat caused 34 percent of business victims to lose revenue and 20 percent even had to cease operations immediately

Executives in the U.S. are disproportionately targeted and 96 percent of U.S. organizations are not very confident in their ability to stop ransomware

SANTA CLARA, Calif. – August 3, 2016 – Malwarebytes™, the leading advanced malware prevention and remediation solution, released [new findings today](#) on the growing threat

<https://www.techtalkthai.com/category/security/>

Central Ohio Urology Group ถูกแฮ็ค ข้อมูลความลับกว่า 223 GB รั่วไหลสู่สาธารณะ

techtalkthai © August 3, 2016 Data Leakage and Data Theft, Security, Threats Update



กลุ่มแฮ็คเกอร์ขบวนการ นามว่า “Pravy Sector” ออกมาเปิดเผยกับทางเว็บไซต์ HackRead ว่าได้ทำการเจาะระบบเซิร์ฟเวอร์ของกลุ่มแพทย์ทางเดินปัสสาวะประจำรัฐโอไฮโอ (Central Ohio Urology Group: COUG) ได้ข้อมูลความลับของห้องแล็บและโรงพยาบาลไปกว่า 223 GB ก่อนอัปโหลดขึ้น Dropbox เพื่อแชร์ออกสู่สาธารณะ

[Read More »](#)

 Like 87

 Tweet

 G+ 1

 Share 2

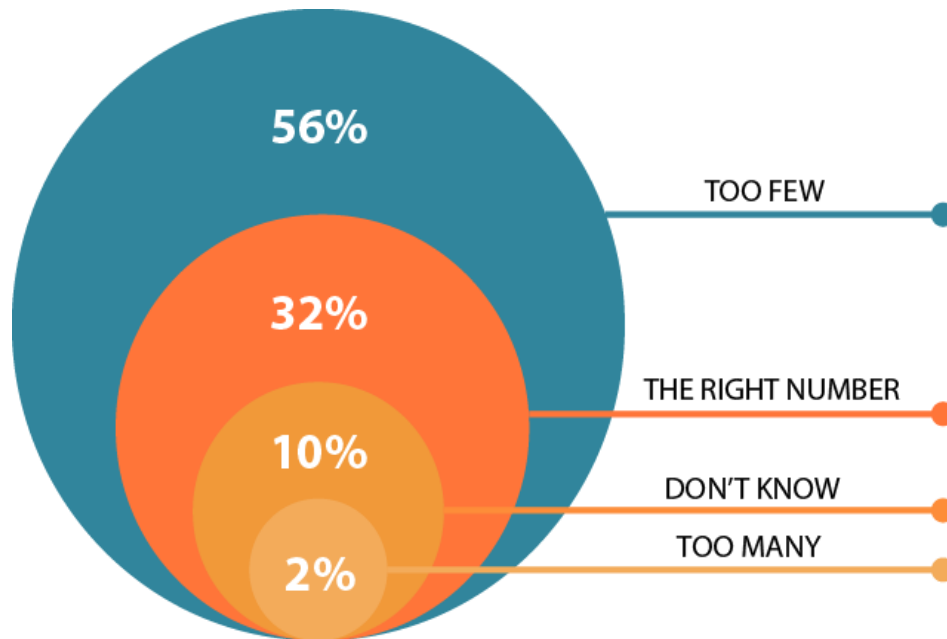
Cybersecurity skills

Cybersecurity professionals must be skilled in technology, business and communication. This includes knowledge of:

- Critical electronic data processes
- Risk analytics
- Information system security

THE CYBERSECURITY SKILLS GAP

Estimated **4.3 million jobs**
available by 2018



Does your organization
have the right number of
security experts?

Source: 2013 Global Information Security
Workforce Study, Frost & Sullivan and Booz
Allen Hamilton

- Cyber is a prefix standing for computer and electromagnetic spectrum– related activities. **The cyber domain** includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications

- Attacks from the informational realm, **where costs are low**, can be launched against the physical domain, where resources are scarce and expensive
- The cyber domain is a complex man-made environment.

- The term cyber attack covers **a wide variety of actions** ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction
- cyber war as a “bloodless war” among states that consists only of conflict in the virtual layer of cyberspace.

Cyberwar

- Responses to cyber war include a form of interstate deterrence (though different from classical nuclear deterrence), offensive capabilities, and designs for network and infrastructure resilience if deterrence fails.
- cyber war and economic espionage are largely associated with states, and cyber crime and cyber terrorism are mostly associated with nonstate actors

Cybersecurity vs. information security

Information security deals with information, regardless of its format. It includes:

- Paper documents
- Digital and intellectual property
- Verbal or visual communications

Cybersecurity is concerned with protecting digital assets. Includes:

- Networks
- Hardware
- Software
- Information that is processed, stored or transported by internetworked IS

PROTECTING DIGITAL ASSETS

Identify

Asset Management

Business Environment

Governance

Risk Assessment

Risk Management

Protect

Access Control

Awareness and Training

Data Security

Information Protection Processes and Procedures

Detect

Anomalies and Events

Security Continuous Monitoring

Detection Processes

Respond

Mitigation

Analysis

Communications

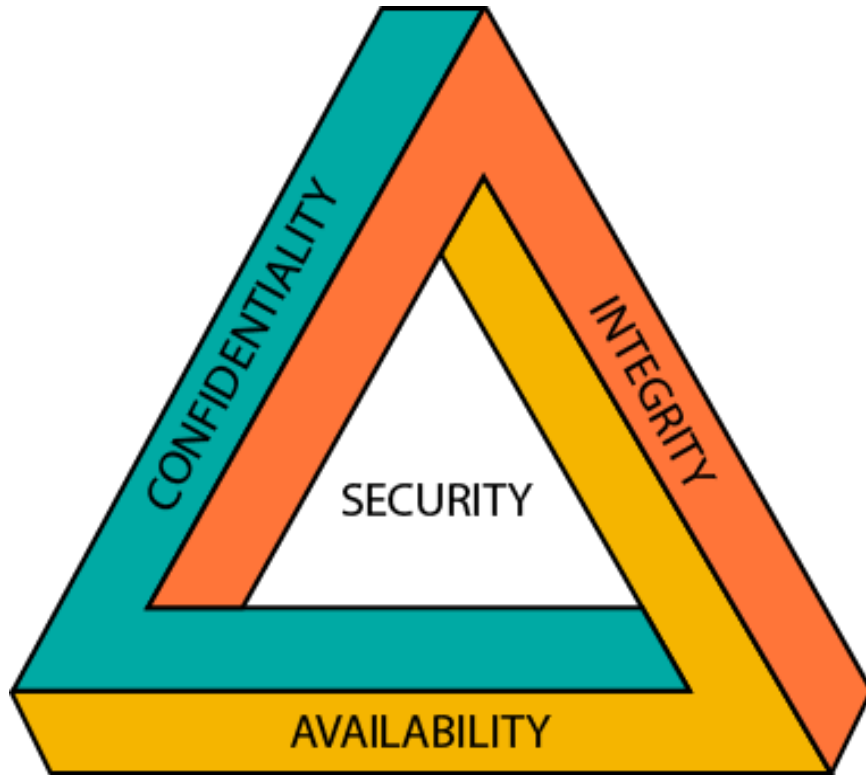
Recover

Recovery Planning

Communications

Continuous Improvements

CONFIDENTIALITY, INTEGRITY & AVAILABILITY



CONFIDENTIALITY

The protection of information from unauthorized disclosure

INTEGRITY

The accuracy and completeness of information in accordance with business values and expectations

AVAILABILITY

The ability to access information and resources required by the business process

GOVERNANCE, RISK MANAGEMENT & COMPLIANCE



RISK MANAGEMENT

The process by which an organization manages risk to acceptable levels

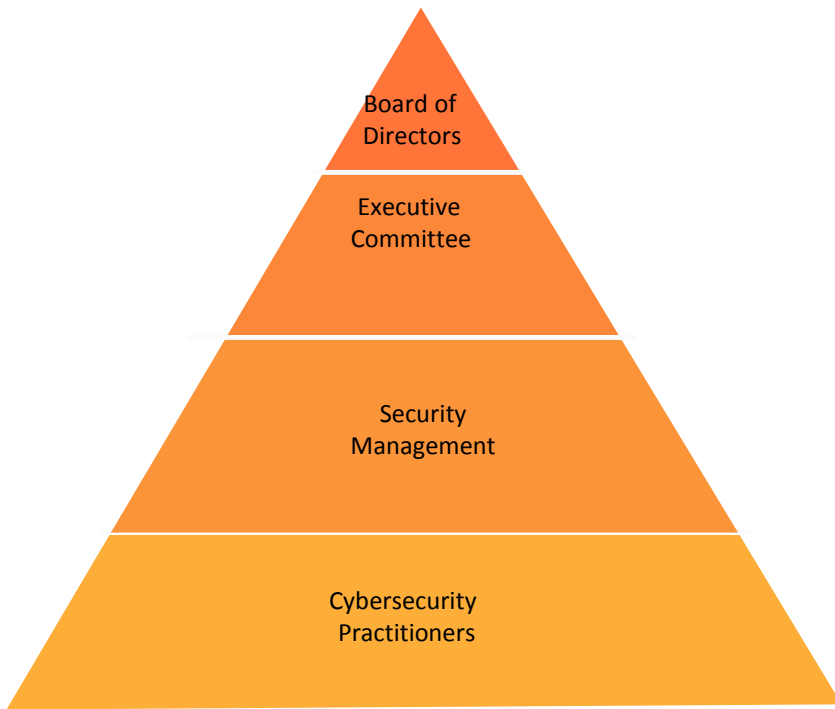
GOVERNANCE

- Provide strategic direction
- Ensure that objectives are achieved
- Ascertain whether risk is being managed appropriately
- Verify that organizational resources are used appropriately

COMPLIANCE

The act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations.

CYBERSECURITY ROLES



BOARD OF DIRECTORS

Identify key assets and verify that protection levels and priorities are appropriate

EXECUTIVE COMMITTEE

Set the tone for cybersecurity management and ensure that necessary functions, resources and infrastructure are available and properly utilized

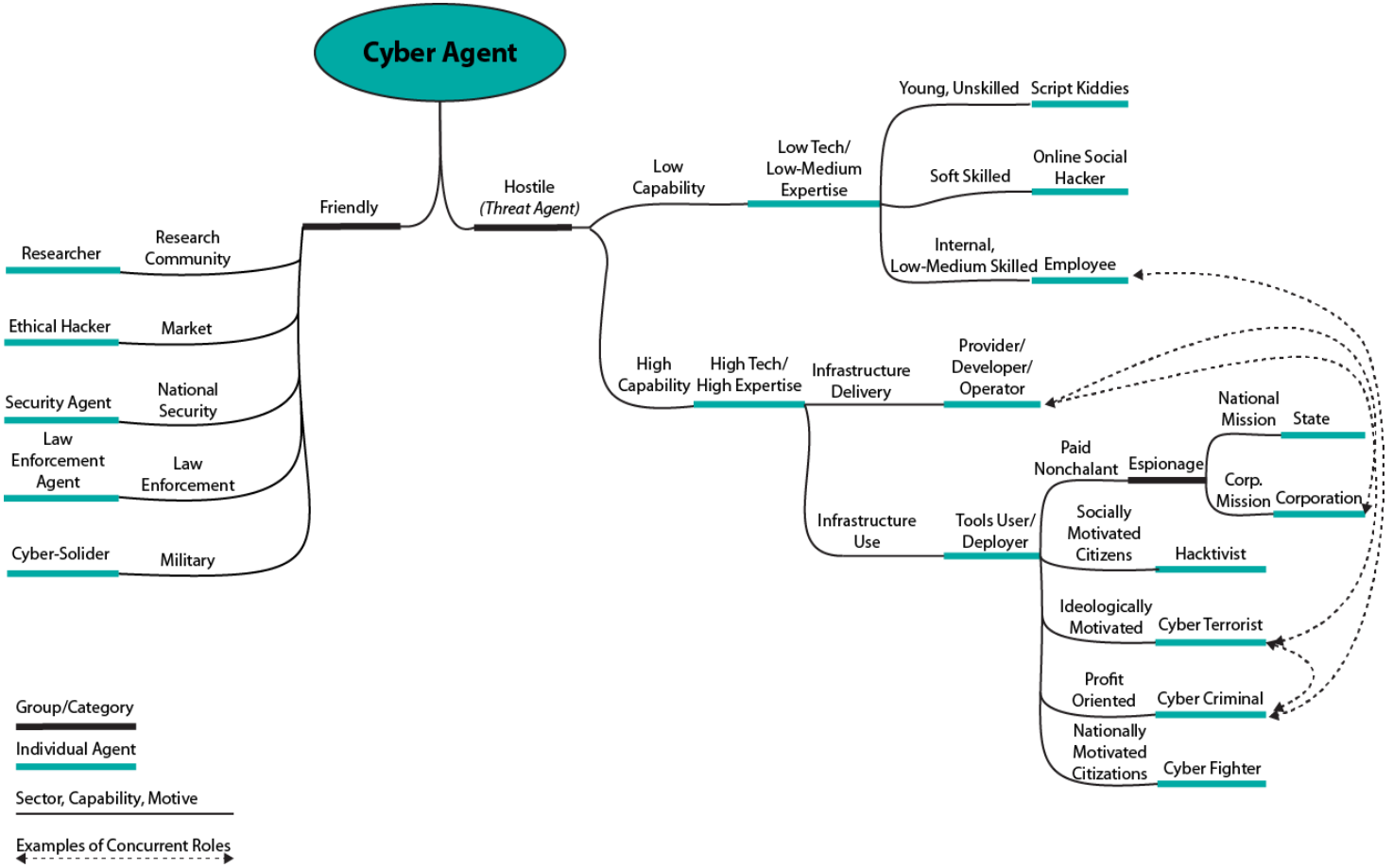
SECURITY MANAGEMENT

Develop security and risk mitigation strategies, implement security programs and manage incidents and remediation

CYBERSECURITY PRACTITIONERS

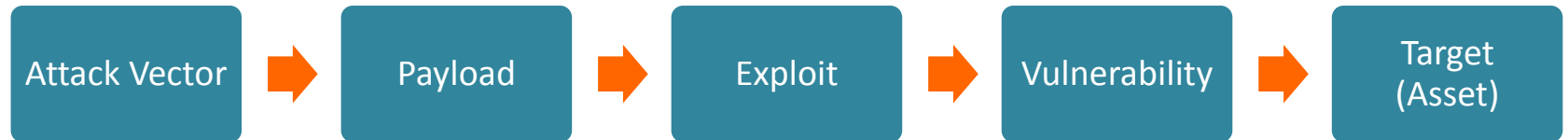
Design, implement and manage processes and technical controls and respond to events and incidents

THREAT AGENTS

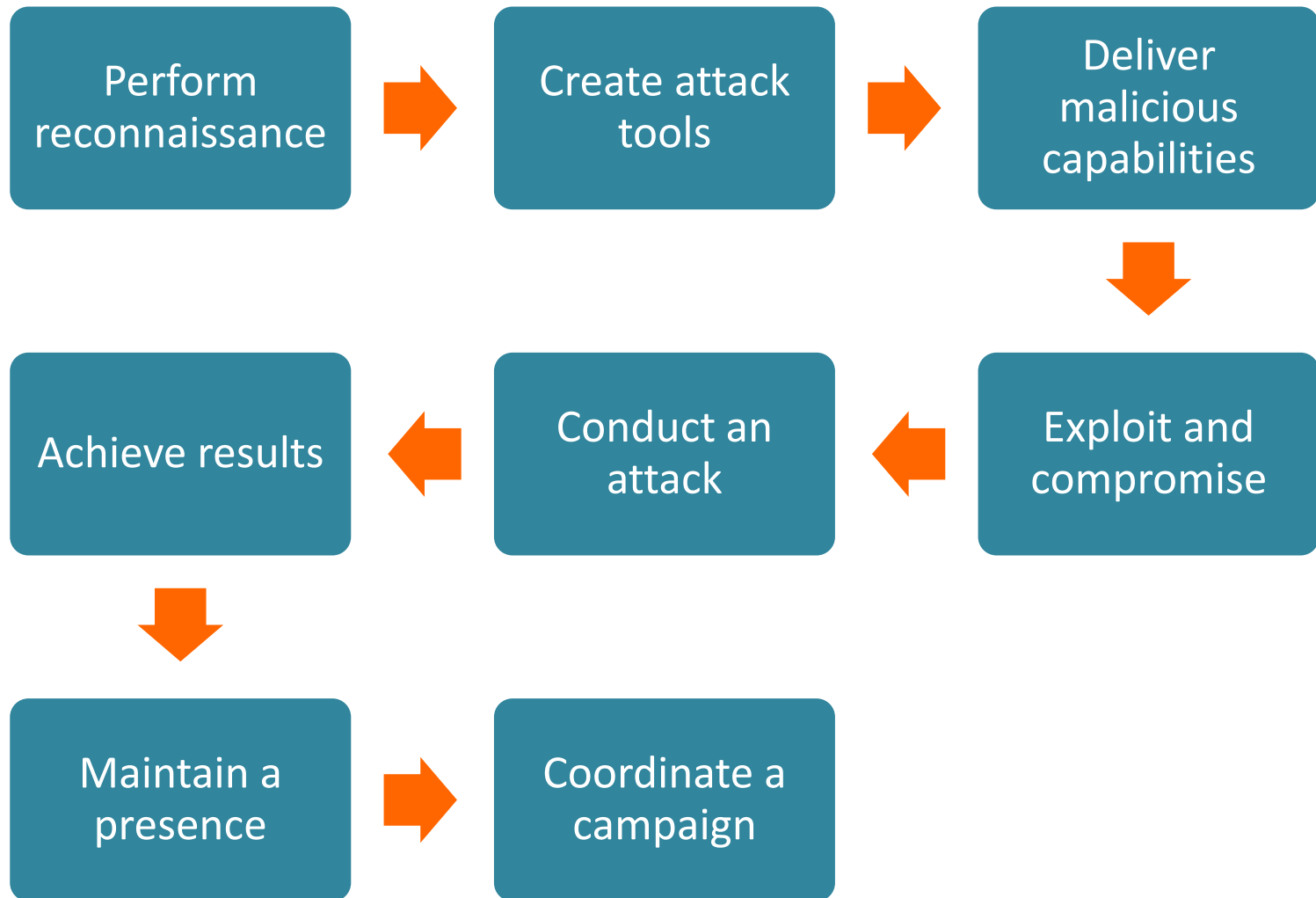


Source: ENISA Threat Landscape 2013

ATTRIBUTES OF A CYBERATTACK



GENERALIZED ATTACK PROCESS



MALWARE & ATTACK TYPES

Virus

Worm

Trojan horse

Botnet

Spyware

Adware

Ransomware

Keylogger

Rootkit

APT

Backdoor

Brute force

XSS

DoS

Man-in-the-middle

Phishing

Spoofing

SQL injection

Zero-day exploit

ISACA Identifies Five Cyber Risk Trends for 2016

- *Internet of Things, ransomware attacks, mobile malvertising, elevation of cybersecurity role are signs of shifting threat landscape*
- Global IT and cybersecurity association ISACA shares **five cyber risk trends for the coming year** that chief information security officers (CISOs) and chief information officers (CIOs) should have on their radar.

Five Key Cybersecurity Trends for 2016

- *“There is no question that cyberattacks are on the rise, but what is changing dramatically is the type of attack and the targets that bold fraudsters are focusing on,”* said Christos Dimitriadis, Ph.D., CISA, CISM, CRISC, international president of ISACA
- <http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx>

1. Cyber-extortion Will Hit Wearables, Medical Devices and Gaming Systems

- 2B use of the Internet of Things (IoT) will more than quadruple by 2020,
- when the worldwide total of connected devices is expected to reach 5.4 billion
- It may be increasingly vulnerable to security risks.
- Nearly three-quarters of IT professionals believe the likelihood of an organization being hacked via an IoT device is medium or high.

- IoT devices are a convenient target for fraudsters, especially those attempting ransomware (a type of malware that denies access to the victim's computer and data until the hacker is paid).
- Since 2012, the number of victimized enterprises—most of them small businesses—agreeing to make ransomware payments has increased from 2.9 percent to 41 percent.²

2.Hackers Will Increasingly Target Cloud Providers

Because more data are shifting outside of organizations through use of hybrid and public clouds,

2016 will bring more attempts from cybercriminals to gain direct access to that information.

In a recent Osterman Research survey, approximately 76 percent⁴ expressed concern about consumer-grade cloud storage, including file sync and share solutions.

3. Millennials Will Care More About Privacy Breaches

- Surveys reveal a shift in thinking among Millennials, who have traditionally valued privacy less than other age groups.
- 2015 marked a number of high-visibility hacks that exposed the personal data of millions; further, Millennials are the generation most likely to use non-traditional IoT devices that are more abundant—and more vulnerable to security risks—than ever. These factors will prompt many Millennials to be more proactive with app providers and other businesses to ensure their private information stays private.

4. Mobile Malware and Malvertising Will Cause Mayhem

- As more services and advertising move from the desktop to mobile devices, 2016 will see a massive increase in the frequency of malvertising (the practice of injecting malicious advertisements into legitimate online advertising networks).
- These and other types of mobile breaches have prompted an overwhelming majority of cyber experts (87 percent) to speculate that mobile payment data breaches will increase over the next 12 months.⁵

5. Cybersecurity Will be the “It” Job of IT

- One of the greatest threats to national and global economic security is the cybersecurity skills gap, and that shortage of experts will continue to stifle CISOs and CIOs in 2016.
- More than half of the global cybersecurity professionals surveyed by ISACA and RSA Conference reported that less than a quarter of job applicants are qualified for the cybersecurity position they are seeking.⁶ Not surprisingly, this challenge has also made cybersecurity a lucrative career option and a “hot” job: it was named #8 on the 100 Best Jobs by U.S. News & World Report.⁷

- According to Robert Stroud, CGEIT, CRISC, past international president of ISACA : “Too few cyber teams are prepared for the new forms of attack. While phishing and malware remain problematic, IT leaders must quickly address new threats tied to IoT, mobile devices, the cloud and other evolving technologies.”

- ISACA offers a wide range of resources on cybersecurity and related issues, and many are free of charge. The organization has also established [Cybersecurity Nexus \(CSX\)](#) to help organizations develop a skilled cybersecurity workforce and help individuals advance their careers through training, guidance, education and credentialing. For more information, visit <https://cybersecurity.isaca.org>.

January 2016 Cybersecurity Snapshot Global Results

- http://www.isaca.org/cyber/Documents/2016-Global-Cybersecurity-Snapshot-Data-Sheet_mkt_Eng_0116.pdf
- Conducted by ISACA, a global association of more than 140,000 IT security, assurance, risk and governance professionals, the January 2016 Cybersecurity Snapshot is based on online polling of 2,920 ISACA members in 121 countries.

1. What do you believe is the likelihood of a cybersecurity attack that disrupts critical infrastructure (e.g., electrical grid, water supply systems) in 2016? $n=2,913$

High	38%
Medium	46%
Low	15%
Unsure	2%

2. Do you believe governments should have backdoor access to encrypted information systems?
 $n=2,907$

Yes	20%
No	63%
Unsure	17%

3. Of the following threats, which THREE are of most concern to your organization in 2016? (Please select up to three.) *n*=2,920

Advanced persistent threat (APT)	39%
DDoS	25%
Ransomware	20%
Social engineering	52%
Watering hole	2%
Insider threats	40%
Malware	30%
Mobile malware	19%
Unpatched systems	31%
Cybercrime	32%
None of the above	1%

4. Are you in favor of regulation requiring companies to notify customers within 30 days of the discovery of a data breach? $n=2,911$

Yes	84%
No	8%
Unsure	9%

5. Of the following, what do you think is the greatest challenge companies would face if they needed to notify consumers of a data breach within 30 days of its discovery? $n=2,913$

Increased cost	11%
Not enough human resources	9%
Systems not designed for this	16%
Concern over corporate reputation	57%
Other	7%

6. Are you in favor of the US Cybersecurity Act of 2015, which encourages cyberthreat information sharing between the private sector and government? *n=2,906*

Yes	57%
No	9%
Unsure	14%
Not applicable to my organization	20%

7. If your organization experienced a breach, do you believe it would voluntarily share cyberthreat information as outlined in the US Cybersecurity Act of 2015? *n=2,903*

Yes	31%
No	16%
Unsure	28%
Not applicable to my organization	25%

9. Does your organization plan to hire more cybersecurity professionals in 2016? *n=2,905*

Yes, and we expect it will be difficult to find skilled candidates	45%
Yes, and we expect it to be easy to find skilled candidates	3%
No	27%
Unsure	25%

10. In general, when hiring new graduates for entry-level cybersecurity positions: *n=2,906*

It is easy to identify who has an adequate level of skills and knowledge.	21%
It is difficult to identify who has an adequate level of skills and knowledge.	63%
Unsure	16%

11. Would you be more likely to hire a cybersecurity job candidate who holds a performance-based certification (i.e., earning the credential requires a direct demonstration of hands-on cyber skills)?

n=2,914

Yes	81%
No	6%
Unsure	13%

12. Has your organization experienced a ransomware incident? (Ransomware is a harmful virus that blocks a user from its computer and demands a fee to return to access.) *n=2,802*

Yes	20%
No	64%
Unsure	16%

15. How has the risk of insider threats (privileged users) changed in your environment since last year (select one)? *n=2,794*

This year has seen a reduced risk	13%
It has not increased	29%
Minimal risk increase	11%
Some risk increase	23%
Significant risk increase	7%
Don't know	13%
Not applicable	3%

16. Which of the following, if any, has been a response to improving security in the virtualized data center (select all that apply)? *n*=2,798

Air gap different types of workloads (sensitive vs non-sensitive)	21%
Adding two factor authentication	44%
Adding dual person approvals for certain actions	29%
Using a password manager for checking in/out password access to systems	23%
None of the above	12%
Not applicable	10%
Don't know	17%

20. Which job title is closest to yours? $n=2,783$

Student	0%
External Consultant	12%
Professor/Teacher	1%
Practitioner	13%
Supervisor	7%
Manager	31%
Director	12%
Vice President	4%
CIO/CISO/CAE	9%
President/CEO	2%
Other	9%

Thank you