

The logo for HIMSS Colombia, featuring the word "HIMSS" in a bold, blue, sans-serif font with a small blue dot above the 'i', followed by "Colombia" in a grey, italicized, sans-serif font.

HIMSS *Colombia*

Bogotá, 27–28 November 2017

Cyber security

Albert Oriol

CIO, Rady Children's



Agenda

- Threat context – Headlines
- What is cyber security
- Key elements of a cyber security program
- How to prevent rodent infestations
- Quick tips

29M

858 public
breaches

records exposed in 2016

\$500B

global cost of cybercrime in 2016

\$4M

\$7M in
the
US

average cost per breach

\$158

\$200 in
the
US

average cost per record

\$5B

global ransomware cost for 2017*

*predicted

75%

of health care industry infected with malware last year

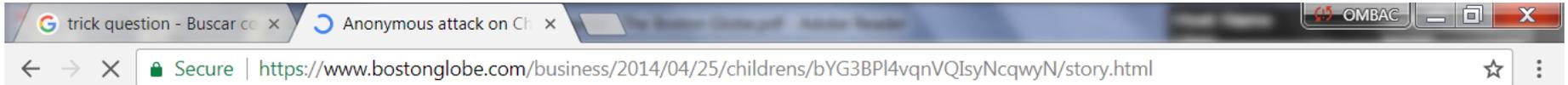
3.5M

x3 cyber criminals

unfilled cyber security jobs by 2021

200

average days attackers stay dormant before detection



Menu
Business
SUBSCRIBE NOW
 Get unlimited access to Globe.com today
Subscribe
Starting at 99 cents
Members Sign In

Anonymous attack on Children's Hospital continues



By **Michael B. Farrell** | GLOBE STAFF APRIL 25, 2014

Top 10 Trending Articles

- | Viewed | Commented | Shared |
|--|-----------|--------|
| | | |
| Elizabeth Warren's family has mixed memories about heritage | | |
| Tufts postpones Scaramucci event after he threatens student and paper with lawsuit | | |
| Here's how Sarah Huckabee Sanders defended | | |

Establishing secure connection...

UNLIMITED access for only 99¢ per week. [Subscribe now](#) →

Password





Attn: Your-150 Dollar Prime Credit Expires on 12/28. Shopper: [REDACTED]

Spam x



Amazon Update <AmazonUpdate@efficaciouscrbays.xyz>

to me ▾

⚠ Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)



The Amazon Marketplace

-----SHOPPER/MEMBER:4726

-----DATE-OF-NOTICE: 12/22/2015

Hello [Shopper: \[REDACTED\]@gmail.com](#)! To show you how much we truly value your years of business with us and to celebrate the continued success of our Prime membership program, we're rewarding you with-\$100 in shopping points that can be used on any item on our online shopping site! (this includes any marketplace vendors)

In order to use this-\$100 reward, simply go below to get your-coupon-card and then just use it during checkout on your next purchase. That's all there is to it!

[Please visit-here now to get your reward](#)

***DON'T WAIT! The Link Above Expires on 12/28!

The screenshot shows a web browser window with the following details:

- Browser Tabs:** "cybersecurity pacemaker" and "Abbott Recalls 465,000 P..."
- Address Bar:** "raps.org/Regulatory-Focus/News/2017/08/30/28370/Abbott-Recalls-465000-Pacemakers-for-Cyber..."
- Page Header:** RAPS REGULATORY AFFAIRS PROFESSIONALS SOCIETY Driving Regulatory Excellence™. Includes "Sign In" and a shopping cart icon with "0".
- Section Header:** "Abbott Recalls 465,000 Pacemakers for Cybersecurity Patch"
- Metadata:** "Posted 30 August 2017" and "By Michael Mezher"
- Text Content:**
 - Medical device maker Abbott on Monday announced it is voluntarily recalling some 465,000 pacemakers to install a firmware update to patch cybersecurity vulnerabilities in the devices.
 - The recall affects six pacemaker models—Accent, Accent MRI, Accent ST, Allure, Anthem and Assurity—that Abbott acquired when it completed its purchase of St. Jude Medical last January.
 - Patients with the devices are being told to speak to their doctors to determine whether they should receive the update, which will require an in-person visit to install.
- Decorative Element:** A vertical graphic of binary code (0s and 1s) on the right side of the article text.

The screenshot shows a web browser window with two tabs. The active tab is titled "Hackers Can Remotely Access Syringe Infusion Pumps" and the address bar shows the URL <https://thehackernews.com/2017/09/hacking-infusion-pumps.html>. The page header features the logo for "The Hacker News" with the tagline "Security in a serious way". Below the header is a dark banner with the text "Es fácil comenzar" and a red button that says "ENCUENTRA MÁS INFORMACIÓN". The main content area displays the article title "Hackers Can Remotely Access Syringe Infusion Pumps to Deliver Fatal Overdoses" and the author "Swati Khandelwal" dated "Saturday, September 09, 2017". At the bottom of the article, there are social sharing buttons for Twitter (49), Google+ (897), Facebook (2.83k), and a generic share button.



PHILIPS

37654-5 Adult

ECG II



Pace Detect Off

SpO₂



♥ /min



120

50

76

PVC 0



mmHg

SYS

160

90

121/81
(94)



off

SpO₂ %

100

90

95

Perf 4.0

👤 /min

30

0

20

T °C

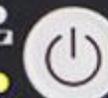
39.0

36.0

37.2

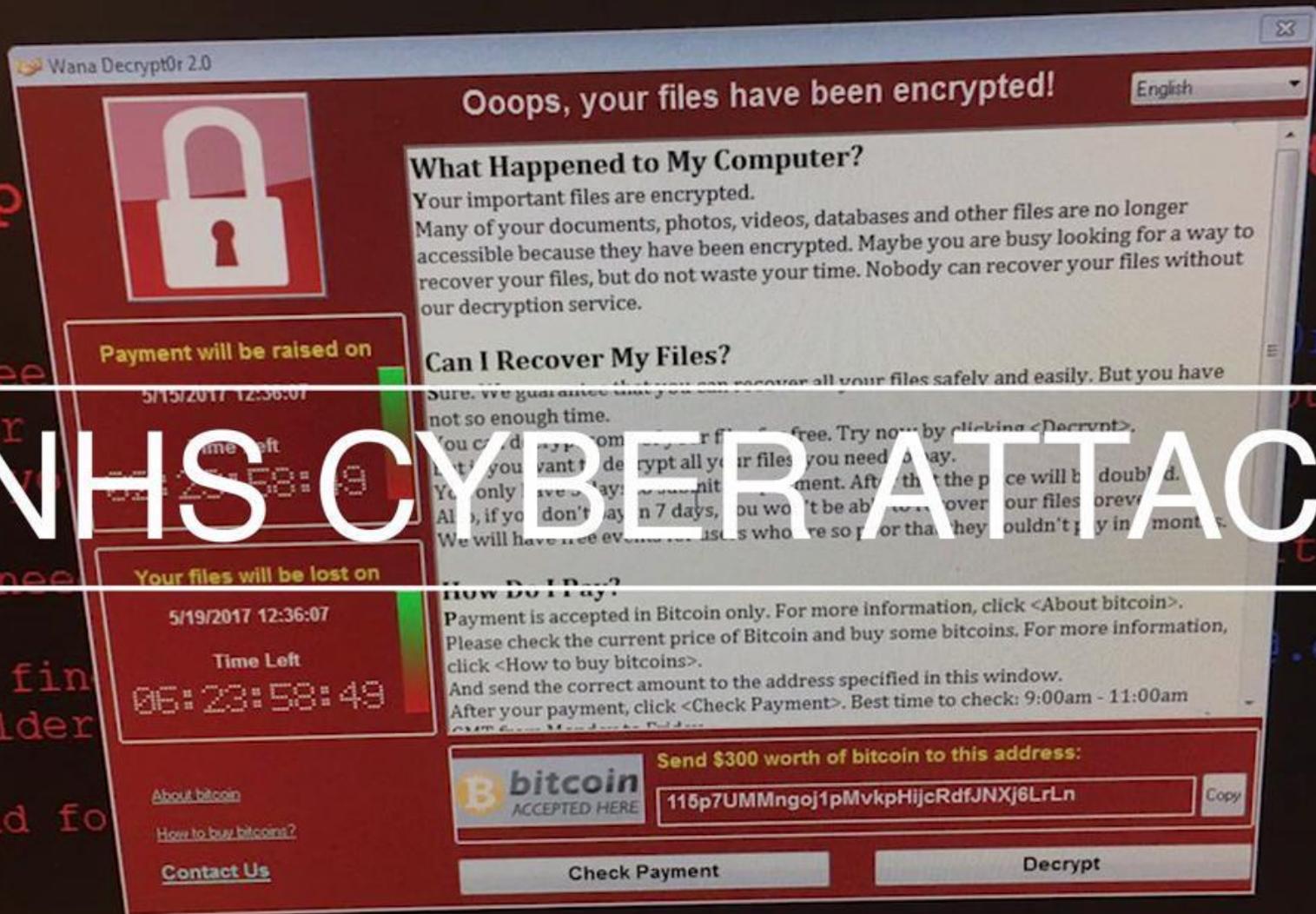


02/01/2006 00:21:43



SureSigns VM6

The screenshot shows a web browser window with two tabs: "ransomware hospitals" and "NHS ransomware cyb...". The address bar displays the URL "www.manchestereveningnews.co.uk/news/greater-manchester-news/nhs-ransomware-c...". The page header features the "Manchester Evening News" logo, social media icons for Facebook, Twitter, and Instagram, a search icon, and a user profile icon. Below the header is a navigation bar with a "LEARN MORE >" button and the "sas" logo. The main content area is titled "NEWS" and features a large headline: "NHS ransomware cyber attack: Full list of hospitals and surgeries affected". Below the headline is a sub-headline: "These are all the NHS trusts affected by the cyber attack". At the bottom of the article, there are social sharing icons for Facebook, Twitter, and Pinterest, with "1322 SHARES". Next to them is a comment icon with "6 COMMENTS". The author information reads "By Alex Pesic" and "19:08, 12 MAY 2017 | UPDATED 19:27, 12 MAY 2017".



NHS CYBER ATTACK

THE DARK ENCRYPTOR

All your files have been encrypted by THE DARK ENCRYPTOR using a military grade encryption algorithm. But don't worry! You can get them back, you just need to pay 100 USD in bitcoin. For more information, please read the text document placed on your Desktop.

Have a nice day !

WARNING: The price will rise to 350 USD if you don't pay in the next 5 days.



Cyber Attack Update: Nuance Still Down, Researchers Believe “Petya” is not Ransomware

June 29, 2017 by Heather Landi

[f](#)
[in](#)
[t](#)
[G](#)
[+](#)
[Reprints](#)


 Nuance Communications, a Burlington, Mass.-based technology company that provides cloud-based dictation and transcription service to hospitals and health systems, continues to be down following the global malware incident on Tuesday that affected multinational companies in at least 65 countries.

Portions of Nuance's network was impacted by the malware incident, which includes a significant part of its services to healthcare organizations. The company is posting updates about the situation to its [website](#). On Wednesday, Nuance said in a web post that it is offering alternative dictation services, specifically [Drupe Medical Group Drupe Medical Network Editing for customers impacted by the Petya malware](#).

ARE YOUR STORY What does it mean to be an INNOVATOR in healthcare today? SHARE YOUR STORY



SC Loss from cybercrime exc x

Secure | <https://www.scmagazine.com/loss-from-cybercrime-exceeded-13b-in-2016-fbi-report/article/671047/>

SC MEDIA

NEWS **CYBERCRIME** NETWORK SECURITY PRODUCT REVIEWS IN DEPTH EVENTS WHITEPAPERS LOG IN • REGIST

THE CYBERSECURITY SOURCE

SC CYBERCRIME

Ransomware Data Breaches APTs/Cyberespionage Malware Phishing Insider Threats

June 26, 2017

Loss from cybercrime exceeded \$1.3B in 2016, FBI report

f t in G+ r

The financial loss from cybercrime in the U.S. exceeded \$1.3 billion in 2016, a rise of 24 percent, according to a new report issued by the Federal Bureau of Investigation's Internet Crime Complaint

FEDERAL BUREAU OF INVESTIGATION

topics eBooks See the lat

MOS

1. US CERT ASLR vulne



What is cyber security?

Cyber security

“The ability to protect or defend the use of cyberspace from cyber attacks (NIST glossary).”

NIST



The screenshot shows a web browser window with a single tab titled "Rady Hospital Apologize: x". The address bar contains the URL "https://timesofsandiego.com/business/2014/06/18/rady-hospital-apologizes-for-data-b...". The main content of the page is a news article with the following elements:

Rady Hospital Apologizes for Data Breach Affecting 20,000 Patients

POSTED BY KEN STONE ON JUNE 18, 2014 IN BUSINESS | 872 VIEWS
0 COMMENTS | [LEAVE A COMMENT](#)

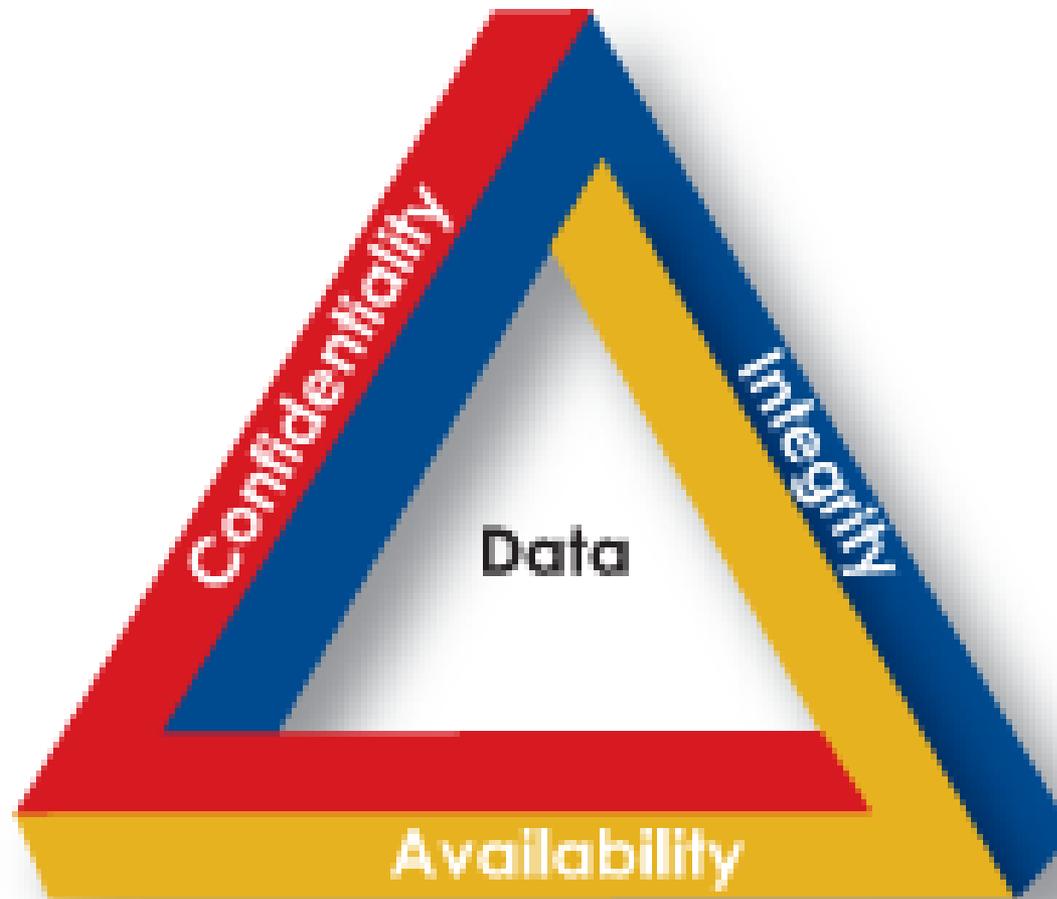
Share This Article:

[f](#) [t](#) [g+](#) [r](#) [p](#) [in](#) [e](#)

Rady Children's Hospital has apologized to the families of 20,000 patients whose private medical data was mistakenly emailed this month and in 2012, according to news reports.



On June 6, U-T San Diego reported, an employee of the Kearny Mesa hospital emailed a spreadsheet that "contained protected information about 14,121 patients to four applicants for data management jobs who subsequently forwarded the document on to two



How can you
achieve cyber
security?

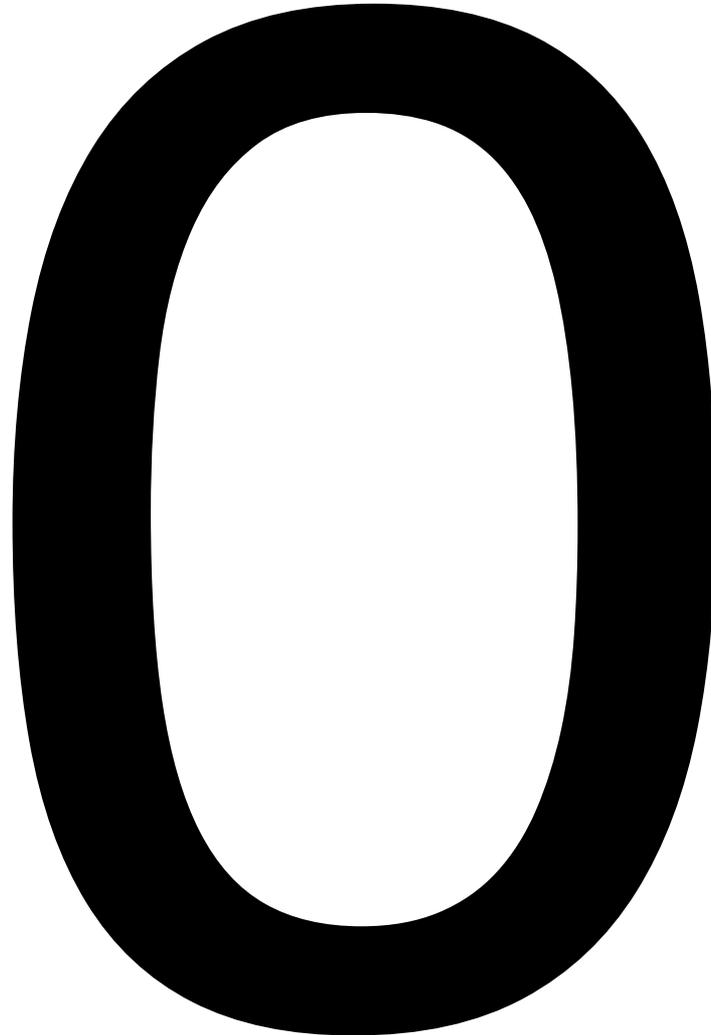
TRICK QUESTION



IT'S A TRAP

What are the key
elements of a good
cyber security
program?





1

Is our organization's cybersecurity program ready to meet the challenges of today's and tomorrow's cyber threat landscape?

The first question addresses *tactical* issues, from a program, (technical) capability, and process perspective, and how they are cascaded throughout the organization. It looks at whether the organization is doing enough due diligence to mitigate risks, depending on its risk profile.

2

What are the new cybersecurity threats and risks, and how do they affect our organization?

The second question addresses *strategic* issues from the business process and corporate objectives standpoint. It is about getting an up-to-date, detailed snapshot of the current cyber threat landscape that is understood by all. It looks at getting comfortable with cybersecurity aspects of core business decisions, cutting through the technical jargon.

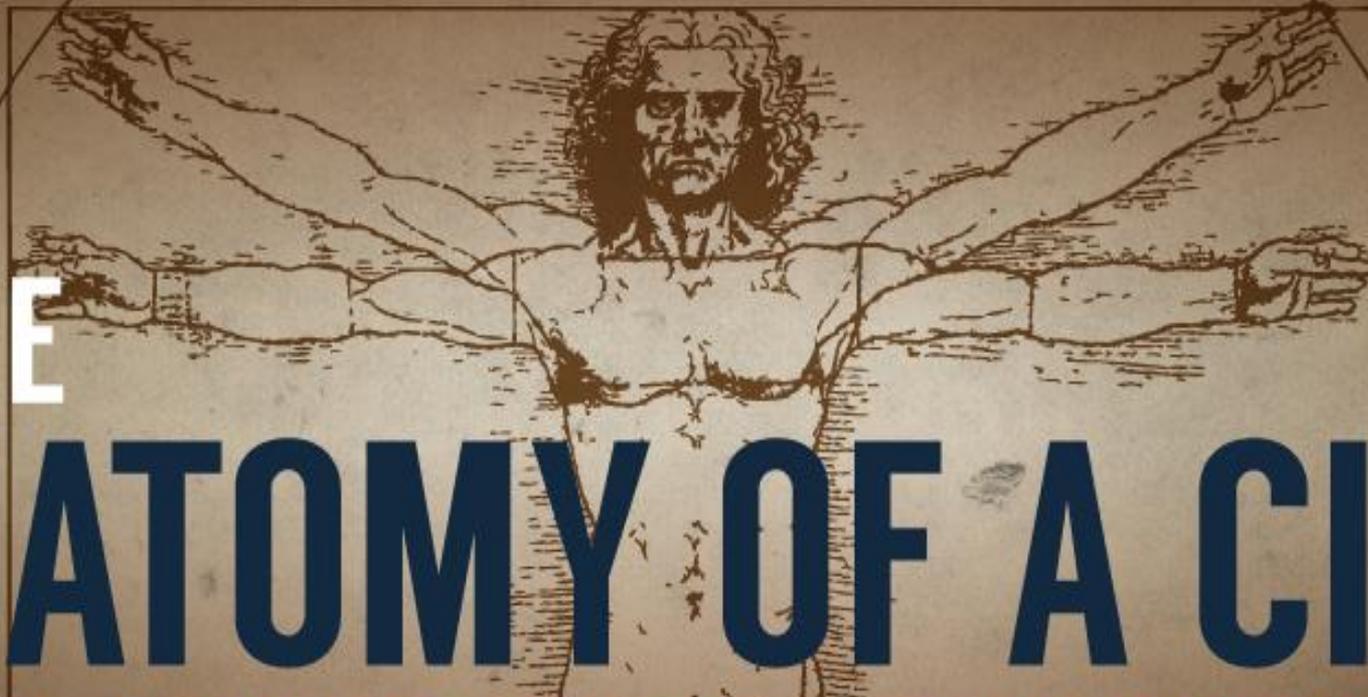
3

What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?

The third question addresses the many *operational* issues, clarifying, prioritizing, and ultimately translating them to what it really means from a risk posture point of view and ultimately, closing the loop. This is "where the rubber meets the road," and indicates how you will know whether you are doing the right thing—so you can sleep at night more easily.







THE

ANATOMY OF A CISO

A BREAKDOWN OF TODAY'S TOP SECURITY LEADERS





Password



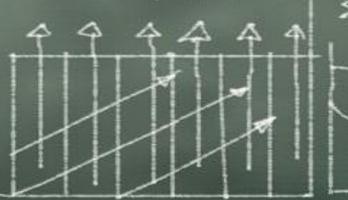
$$\text{€}^2 \circ \left(\frac{1271}{31} \right) + 44 \left(\frac{01,27}{31} \right) + \$2\sqrt{H_0}$$

The chalkboard is densely packed with handwritten content. On the left, there are several small bar charts and a line graph. In the center, a man in a dark suit stands with his back to the camera, looking at the board. The board itself is covered in various mathematical and financial notations. At the top left, there is a large equation involving currency symbols and fractions. Below it, there are smaller equations and symbols like €^2 , $\text{\$}$, and H_0 . In the middle, there are several graphs, including a bar chart with four bars of increasing height, a line graph with multiple curves, and a diagram with a circle and arrows. On the right side, there is a table with columns labeled € and $\text{\$}$, and rows of numbers and symbols. At the bottom right, there is a diagram with a box labeled 'data' and arrows pointing to it. The overall scene suggests a complex financial or mathematical analysis being presented or reviewed.

$$319211$$
$$721132(1) p_0 f L_0$$
$$123012770$$

$$\text{€}^2(213H10)H$$
$$72(00|0 \frac{1}{2})342$$

\$\$\$\$\$\$\$\$

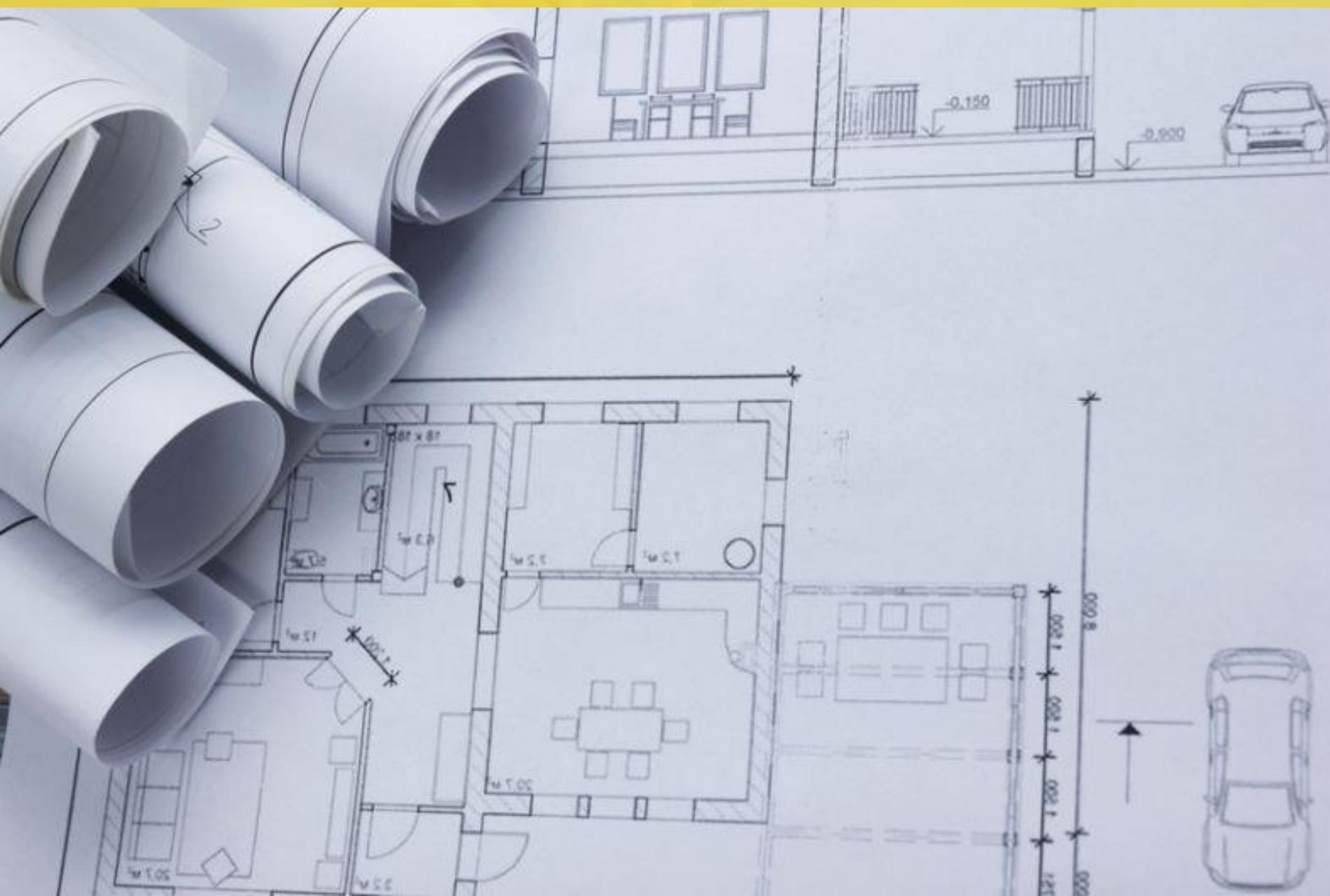


101101010	
1011101	
1110011	
10011104	
1011001	
7201124	
70910	

???	€	\$\$
...		

720	€ + \$ + a
3121	- □ -
data	□































CONSIDERE

a su Mascota

ANTES

de Usar

VENENO

para

RATAS







quick
TIPS

















HIMSS Colombia

Bogotá, 27–28 November 2017



¡Muchas Gracias!

Albert Oriol
Rady
Children's

Hospital
San Diego

aoriol@rchsd.org

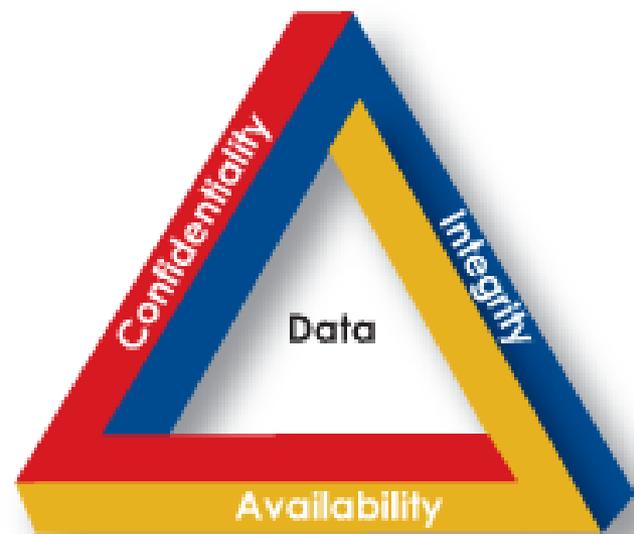
+1 858 966 5924

@RadyCIO 

APPENDIX

What Is Information Security?

- Vigilance
- Knowledge
- Risk Management
- Methodology and Policies
- Applied Science/Forensics
- Architecture
- Implementation
- Operations
- Awareness training



Policies and Procedures

- Account provisioning and de-provisioning
- Classification (public, restricted, sensitive), storage and transmission of information
- What to encrypt and when
- When and how to apply patches
- Software development, code promotion, change management and hardware configuration
- Event monitoring, incident response, backups, restore, disaster recovery and business continuity
- Assigned responsibility for InfoSec
- End user training
- Sanctions

Layered Defense

- Policies and procedures
- Network segmentation
- Firewalls
- IDS/IPS
- DLP
- Encryption
- Integrity checkers
- Content filtering
- Log aggregation
- Event Correlation
- Antimalware
- Vulnerability scanner
- Two factor authentication
- Incident response
- Awareness training
- Cyber insurance

The Seven Common-Sense Rules of Information Security

1. Don't provide insecure access to interesting data.
2. Manage vulnerabilities. Verify compliance with security standards and regulations.
3. Don't provide "nests" for hackers. Ensure InfoSec policies/procedures are solid.
4. Set traps to detect intrusions.
5. Monitor reports generated by your security monitoring tools.
6. Learn about security standards and operations.
7. Vigilantly look for unusual activity.

Standards: Our Guiding Sunlight in the Cloud

- Ensures a comprehensive approach.
- Provides “external world” standard for measurement.
- Establishes best practices for technology and operations.
- May be required by law/mandate/contract.

NIST SP 800-53A

- NIST Special Publication 800-53 is part of the series that reports on the Information Technology Laboratory's (ITL) research, guidelines, and outreach efforts in information system security, as well as on ITL's activity with industry, government, and academic organizations.
- Provides a comprehensive set of controls for the confidentiality, integrity, and availability of a system and the information it stores.
- Required for FISMA compliance, but also represents a good overall application/system security standard.

ISO 27001

- Published by the International Organization for Standardization (ISO) as *Information technology - Security techniques - Code of practice for information security management*.
- Provides overall infrastructure and environment best-practice recommendations.
- More focused on infrastructure and organizational layers than application security.