Information Security & Privacy:

Making a Critical Coexistence

HIMSS

CENTRAL & SOUTHERN OHIO Chapter

Copyright © 2010 R.J. Romero. www.hipaacartoons.com

"Your test results were accidentally faxed to a veterinarian. He recommends a de-wormer."

Defining the space:

- **Privacy defined:**
  1. The HIPAA Privacy Rule – Establishes national standards to protect individuals medical records and other personal health information and rights for the individual to examine, request corrections, and obtain a copy of their health records.
     - Defines when health information is “identifiable” and therefore protected.
     - Requires appropriate safeguards to protect the privacy of personal health information.
     - Sets limits and conditions on the uses and disclosures of such information without patient authorization.

  2. Dictionary.com Rule– #3. Freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one’s personal data or information as by a government, corporation, or individual.

Defining the space:

- **Information Security:**

  “The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.” (Wikipedia)

  - ➢ **C**onfidentiality (Privacy)
  - ➢ **I**ntegrity (Quality/Accuracy)
  - ➢ **A**vailability (Accessibile)

- **Covered information:**

  1. PHI (Protected Health Information)
  2. PII (Personally Identifiable Information)
  3. Sensitive business data
  4. Big data

The Why:

- **Information Security and Privacy importance:**
  1. Our patients, employees, and partners entrust us to be good stewards of their sensitive information.
  2. Integrity and availability of data is absolutely critical when patient health and safety come into play.
     - ➢ Imagine… The EHR virus!!!
     - ➢ Ransomware
       - Hollywood Presbyterian
       - MedStar
       - Methodist Hospital
  3. Defense against identity theft… The opportunity for large payoffs to cybercriminals is huge.
     - ➢ ‘Medical records are more valuable because they can be used to create identities and carryout sophisticated insurance fraud schemes’

Healthcare cybersecurity challenges in an interconnected world // Key findings from The Global State of Information Security® Survey 2015
www.pwc.com/gsiss2015 // ***www.pwc.com/cybersecurity***

The Why:

- **Information Security and Privacy importance (cont.):**

4. Reputation and future business outlook is, in part, dependent on maintaining good Information Security and Privacy.

5. The penalties for lack of compliance are significant.

➢ HIPAA (OCR) Criminal and Fines

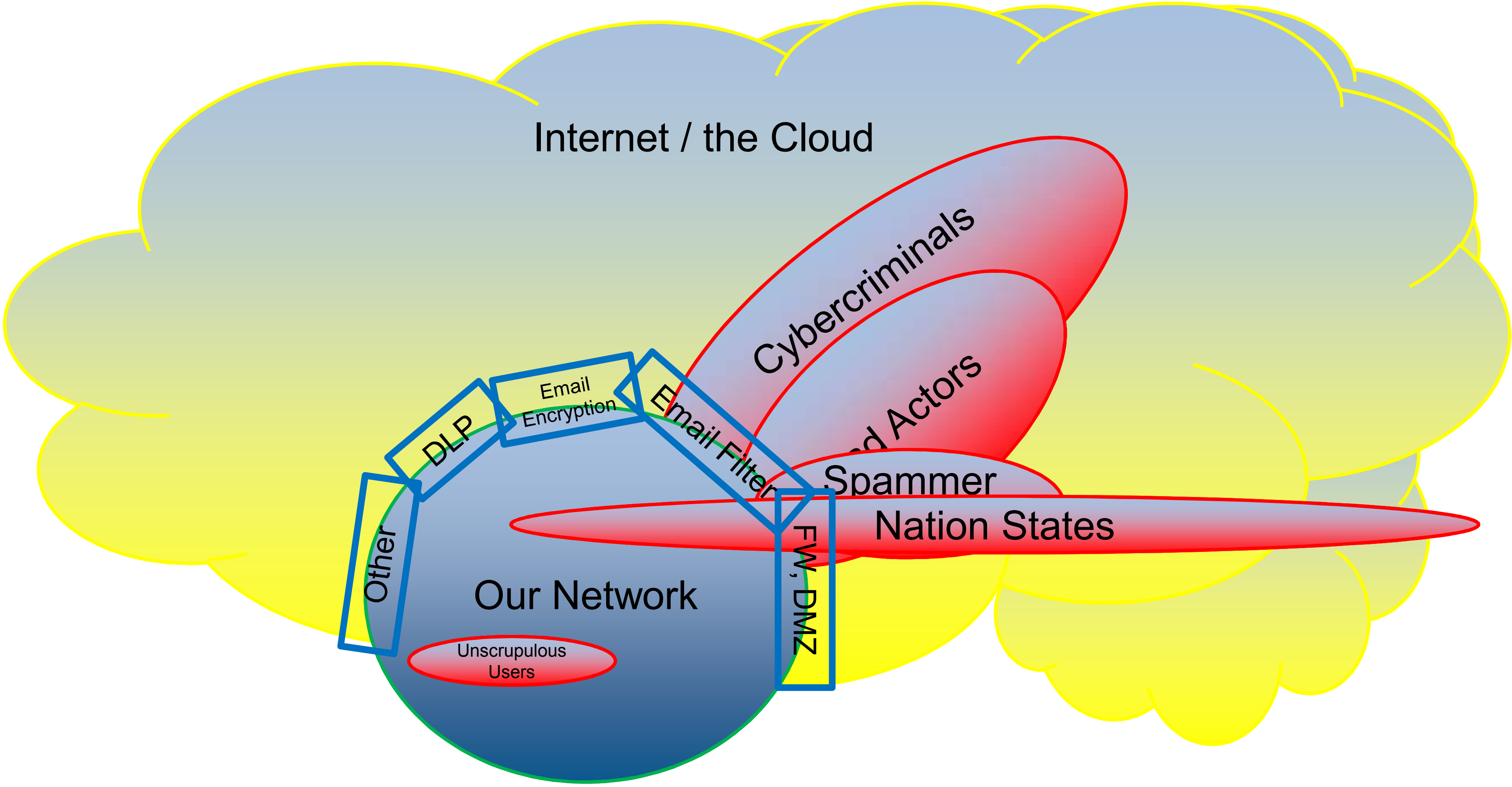
- St Elizabeth Medical Center (MA) fined $218K + Corrective Action Plan for storage of ePHI on unsecured Internet storage platform. HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications - June 10, 2015
- Lahey Hospital and Medical Center - $850K + Corrective Action Plan for Unsecured / Improper use of Medical Devices and workstations – November 2015
- New York and Presbyterian Hospital and Columbia University fined $4.8M for joint breach. http://www.hhs.gov/news/press/2014pres/05/20140507b.html
- Alaska Behavioral Health Service fined $150K + Corrective Action Plan. HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software

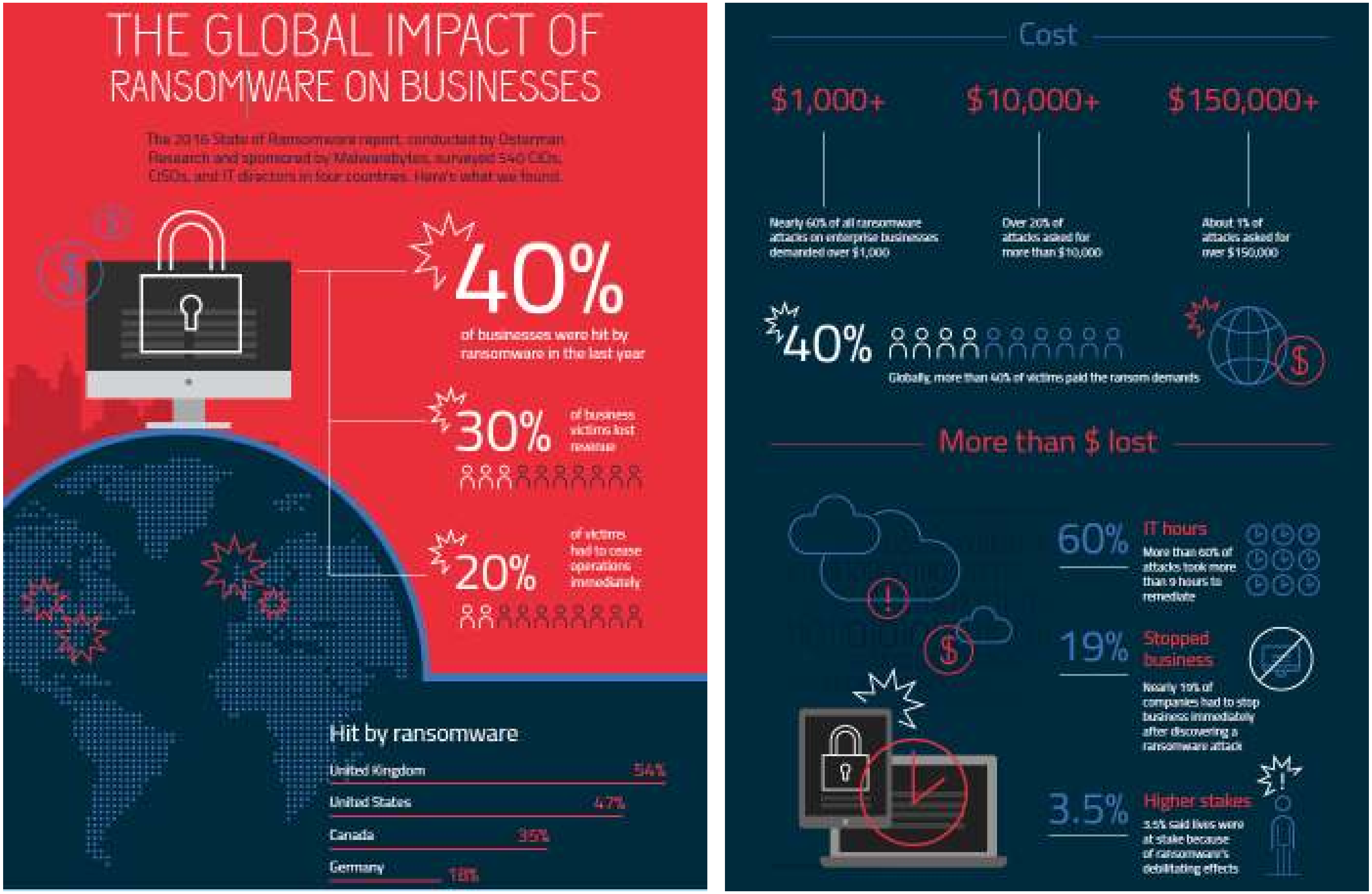
➢ Cost to defend and preserve

- **The evolutionary use of security technology…**

What is predicted to be the biggest threat to data CIA for 2016?

A. Hackers B. Internal Users C. Ransomware





THE GLOBAL IMPACT OF RANSOMWARE ON BUSINESSES

The 2016 State of Ransomware report, conducted by Osterman Research and sponsored by Malwarebytes, surveyed 540 CIOs, CISOs, and IT directors in four countries. Here's what we found.

40% of businesses were hit by ransomware in the last year

30% of business victims lost revenue

20% of victims had to cease operations immediately

Hit by ransomware

United Kingdom	54%
United States	47%
Canada	35%
Germany	18%

Cost

$1,000+ Nearly 60% of all ransomware attacks on enterprise businesses demanded over $1,000

$10,000+ Over 20% of attacks asked for more than $10,000

$150,000+ About 1% of attacks asked for over $150,000

40% Globally, more than 40% of victims paid the ransom demands

More than $ lost

60% IT hours More than 60% of attacks took more than 9 hours to remediate

19% Stopped business Nearly 19% of companies had to stop business immediately after discovering a ransomware attack

3.5% Higher stakes 3.5% said lives were at stake because of ransomware's debilitating effects

Global Impact of Ransomware on Business 2016, Malwarebytes
http://go2.malwarebytes.com/DUxh00z0GSY00616Iu3F0nR

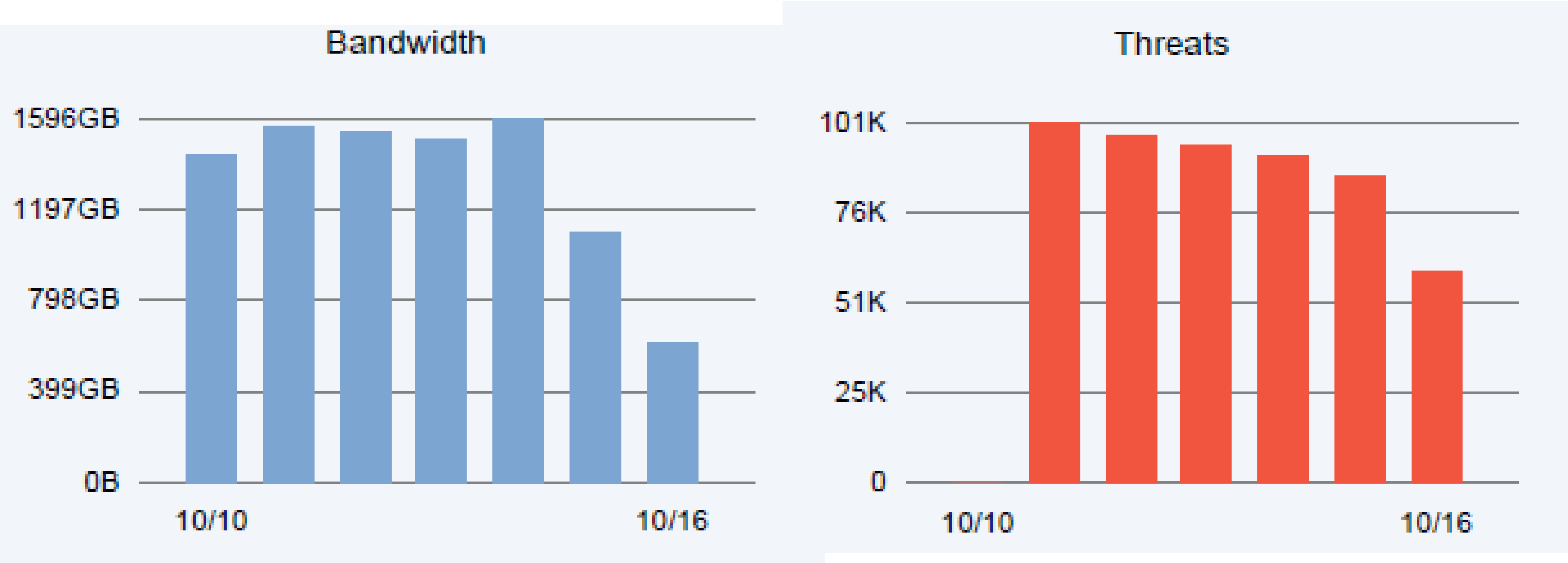
- **The use of technology**

  With enough technology and tools we can protect data_______.

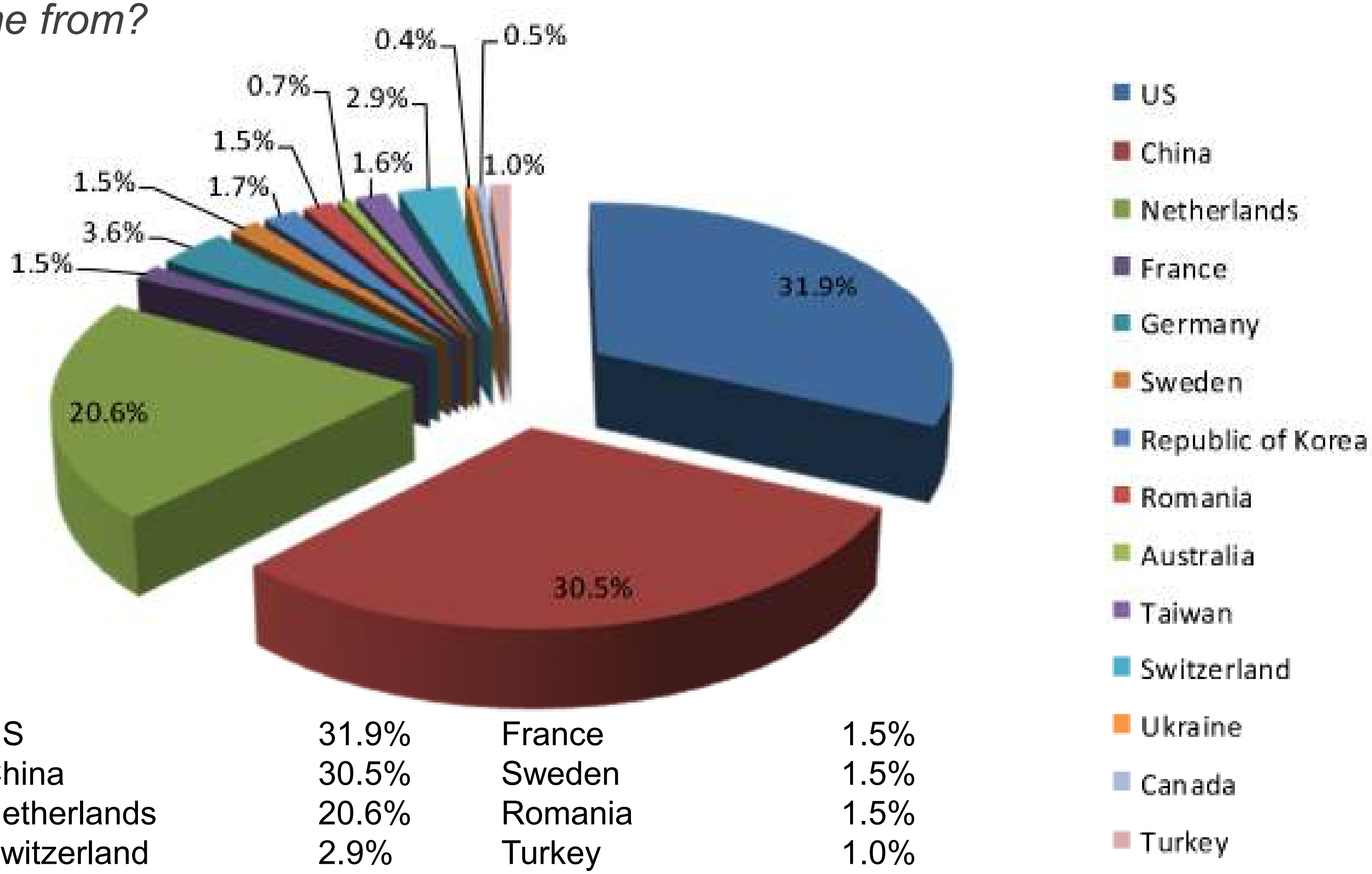
  A. All of the time *B. Most of the time*

  C. Some of the time *D. None of the time*

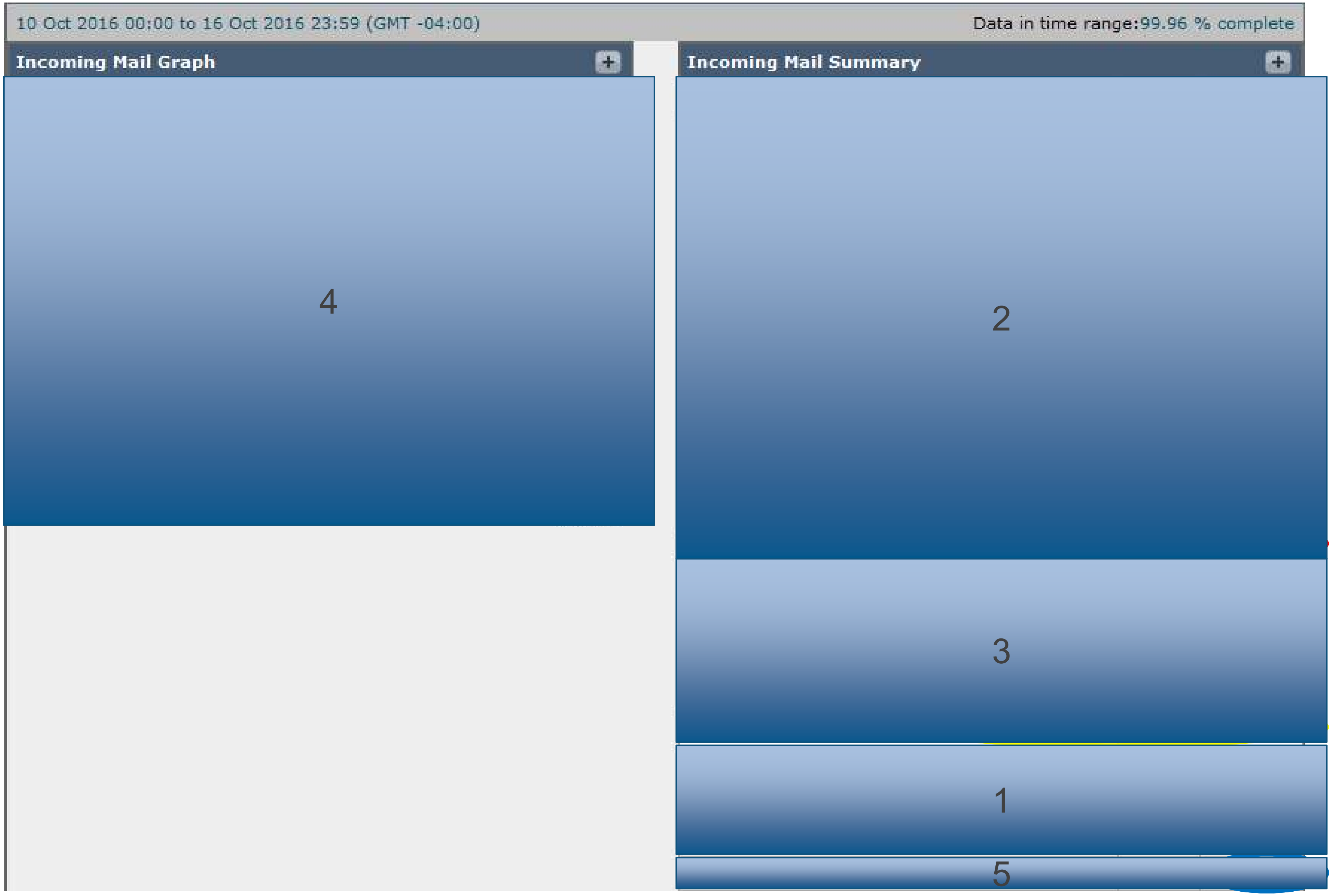
The overwhelming odds… What does the average organization face?



The overwhelming odds… Where do the bad guys (threat actors) come from?



US	31.9%	France	1.5%
China	30.5%	Sweden	1.5%
Netherlands	20.6%	Romania	1.5%
Switzerland	2.9%	Turkey	1.0%
Germany	3.6%	Australia	0.7%
Republic of Korea	1.7%	Canada	0.5%
Taiwan	1.6%	Ukraine	0.4%

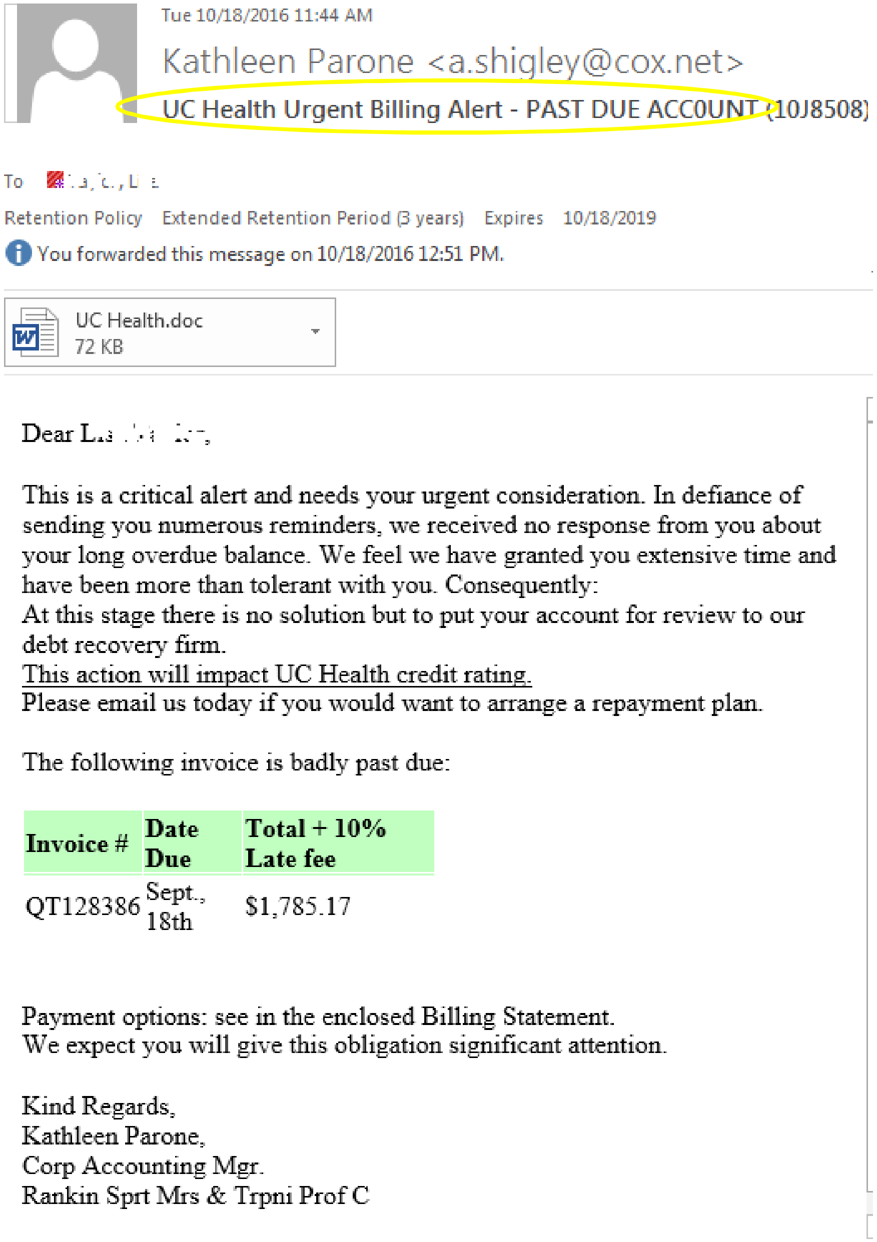


10 Oct 2016 00:00 to 16 Oct 2016 23:59 (GMT -04:00)

Data in time range:99.96 % complete

Incoming Mail Graph

Incoming Mail Summary



Tue 10/18/2016 11:44 AM

Kathleen Parone <a.shigley@cox.net>

UC Health Urgent Billing Alert - PAST DUE ACC0UNT (10J8508)

To [redacted]

Retention Policy Extended Retention Period (3 years) Expires 10/18/2019

You forwarded this message on 10/18/2016 12:51 PM.

UC Health.doc
72 KB

Dear [redacted],

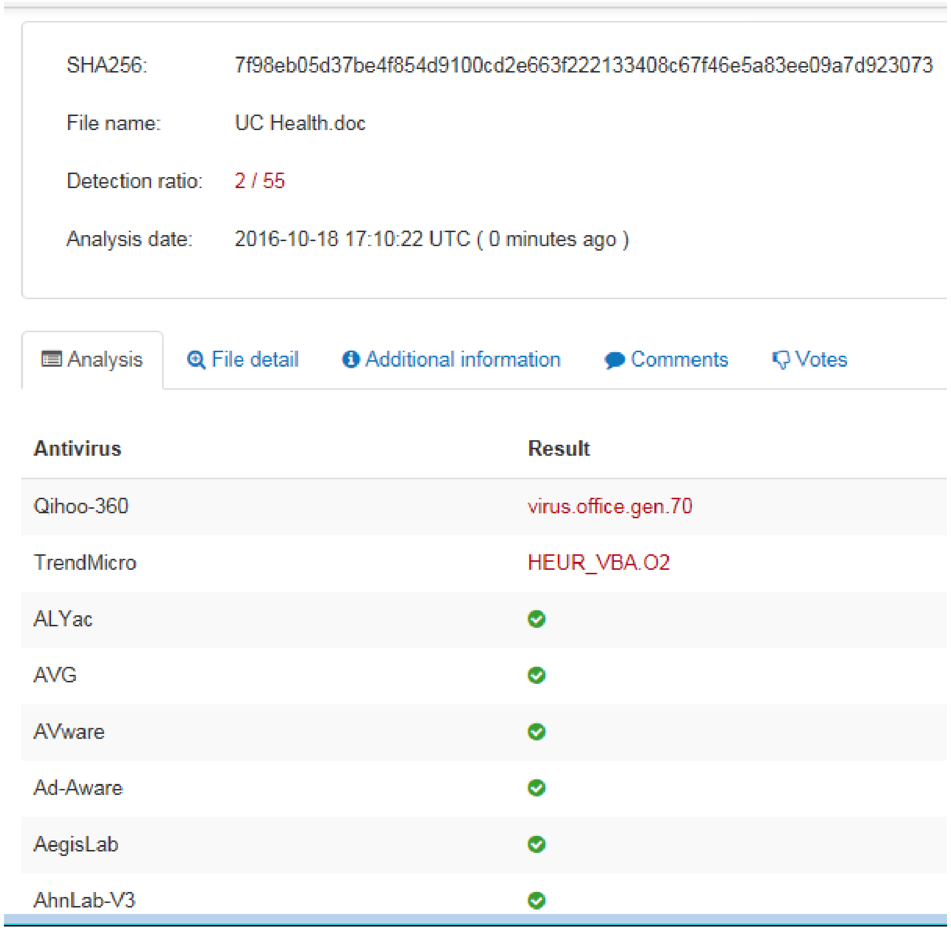
This is a critical alert and needs your urgent consideration. In defiance of sending you numerous reminders, we received no response from you about your long overdue balance. We feel we have granted you extensive time and have been more than tolerant with you. Consequently:
At this stage there is no solution but to put your account for review to our debt recovery firm.
This action will impact UC Health credit rating.
Please email us today if you would want to arrange a repayment plan.

The following invoice is badly past due:

Invoice #	Date Due	Total + 10% Late fee
QT128386	Sept., 18th	$1,785.17

Payment options: see in the enclosed Billing Statement.
We expect you will give this obligation significant attention.

Kind Regards,
Kathleen Parone,
Corp Accounting Mgr.
Rankin Sprt Mrs & Trpni Prof C



SHA256: 7f98eb05d37be4f854d9100cd2e663f222133408c67f46e5a83ee09a7d923073

File name: UC Health.doc

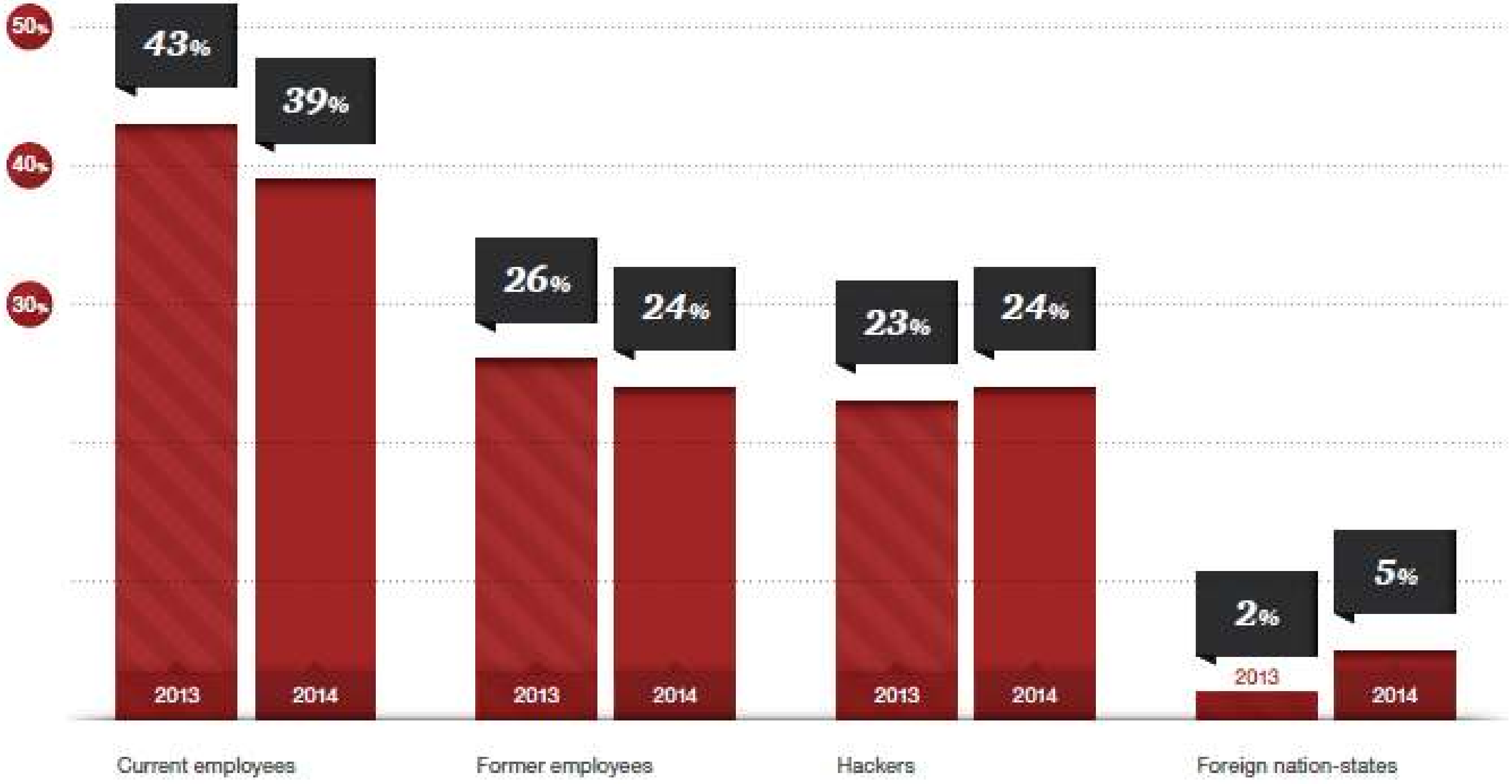
Detection ratio: 2 / 55

Analysis date: 2016-10-18 17:10:22 UTC (0 minutes ago)

Antivirus	Result
Qihoo-360	virus.office.gen.70
TrendMicro	HEUR_VBA.O2
ALYac	✓
AVG	✓
AVware	✓
Ad-Aware	✓
AegisLab	✓
AhnLab-V3	✓

- **Some recent national statistics…**

Sources of Incidents (All Survey Respondents):



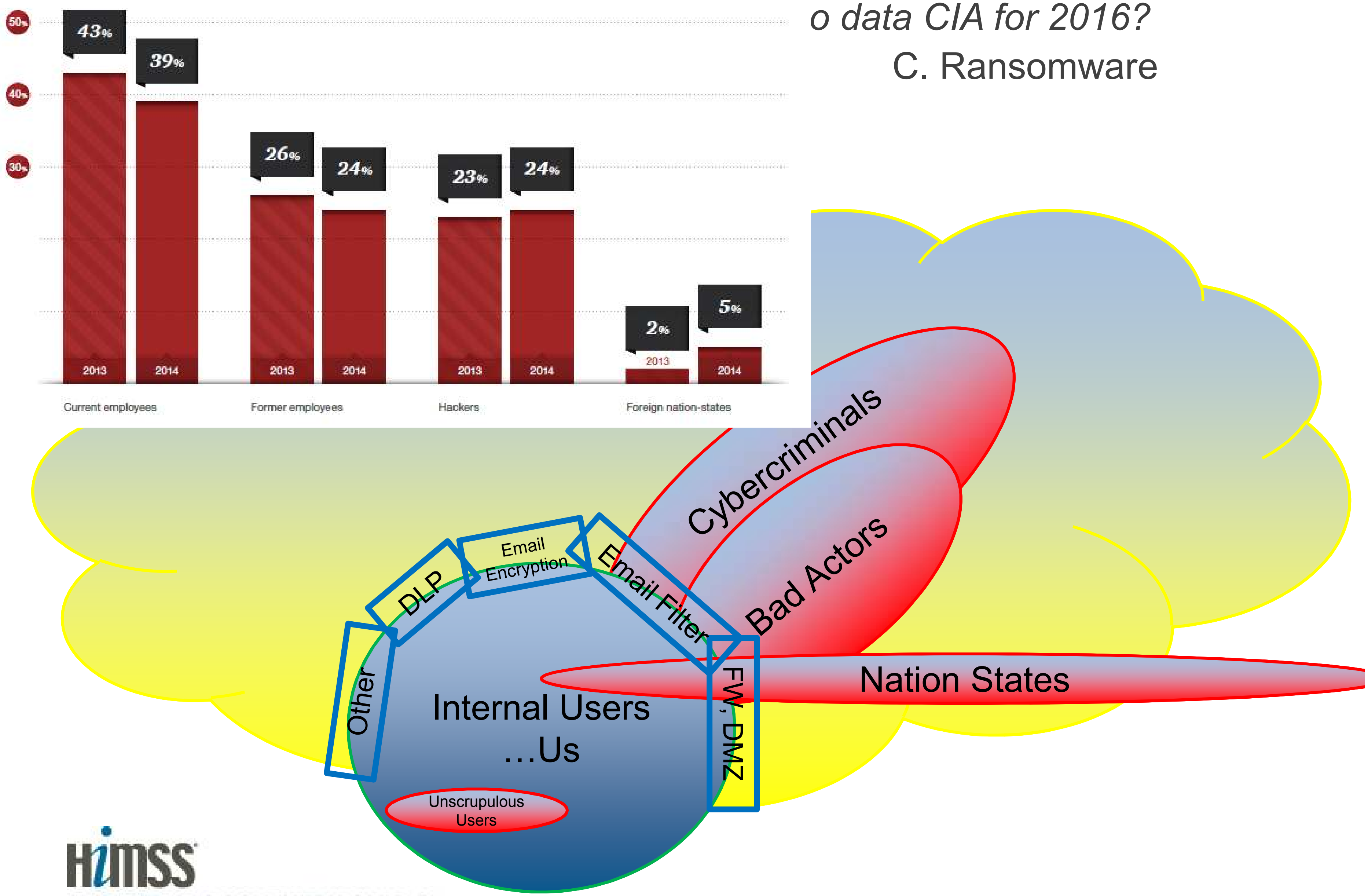
Healthcare cybersecurity challenges in an interconnected world // Key findings from The Global State of Information Security® Survey 2015
www.pwc.com/gsiss2015 // ***www.pwc.com/cybersecurity***

HIMSS CENTRAL & SOUTHERN OHIO Chapter

- **The evolutionary use of security technology…**

o data CIA for 2016?

C. Ransomware



The How:

- **How is Information Security & Privacy accomplished… *Education, Understanding, Acceptance… <u>PRACTICE</u>***
- **A Partnership for Success**

1. Information Security and Privacy have to be on the same page.
   - ➢ OCR Guidance
   - ➢ Rounding - EOC
   - ➢ Contracting – BAA, Security Terms, Vendors
   - ➢ Policies and Procedures
2. Not done alone – need boots on the ground, every user is eyes & ears
3. Desire open / honest communication – the door is always open
4. "Did I do thaaat???" Everyone is an Urkel… We WILL make mistakes!
   - ➢ **"90% of security incidents are still caused by PEBKAC and ID10T errors", according to Verizon's 2015 Data Breach Investigations Report**
   - ➢ No penalty for self reporting of accidental, unintentional, or unintended acts
5. Continue to educate and inform your users

Education Pointers:

- **Top Do’s and Don’ts**

1. Safe passwords… The 4P’s1$4Me
   - ➢ “Pr0per PA$$w0rd$ Pr0tecT PH!”
   - ➢ UC, LC, Special Characters, Numbers
   - ➢ Don’t: Post-it ®, tape it, share it, email it, or text it

2. The Encryption Prescription… Be hip and encrypt!
   - ➢ PHI? PII? Sensitive Data? - ENCRYPT
   - ➢ Email
     - - Use your company’s encryption
     - - Don’t forget replies… check the thread
     - - Are your recipients correctly spelled including the domain?
   - ➢ Smartphone – If it will have PHI on it, it HAS to be encrypted
     - - Android vs. iOS (Apple iPod/iPad) vs. MS
     - - Texting PHI is not permitted without an approved app
   - ➢ Desktops & Laptops/Mobile Devices– All endpoints should be encrypted
   - ➢ The Cloud…

Education Pointers:

- **Top Do's and Don'ts (cont.)**

3. Email Safety: **Think, before you Link…**
    - ➢ A Beta Eta the Data, You are the Alpha and Omega… something seems Phishy???
    - ➢ The fly over and hover cover:

      http://this.looks.safe.com/ - But Do NOT Click or…

      http://not.really.safe.com.but.UNSAFEEEE.com
    - ➢ Attachments & Links – Never open / click unless you are sure of the source.

4. The device Battle Royale… BYOD vs. POCD vs. NOCD
    - ➢ Bring Your Own Device vs Personally Owned Computing Device – whether you bring it or not
    - ➢ NOCD - Not Owned Computing Device (Libraries, Kiosks, Friends)
    - ➢ All devices not managed or owned by organization

Education Pointers:

- **Top Do's and Don'ts (cont.)**

5. Internet – It's like the X-Files, "Trust No One"
   - ➢ Safety Tips and Tricks

6. The paper caper…
   - ➢ Is it PHI, PII, or just an old printout with useless data?

   >>>> No matter what. "If it's paper… Shred It!" <<<<

7. Lockout or Logout – Either/Or but <u>never</u> Neither/Nor
   - ➢ Whether to lockout or logout depends on where you are and your time away from the computer
   - ➢ Timeout your personal computer with screen saver lockout

Coexistence Means:

- **Making it work**

1. Takes time to build a relationship with and between IT, Privacy, Legal, HR, and others. Cultivate it.
2. Recognize you will rely on each other to support one another
3. Accept there will be bumps in the road
4. Focus on learning and educating
5. Set realistic expectations and common goals for success
6. Lead by example – Live by the standards you want to set

- **Questions?**