IBM Security

Intelligence. Integration. Expertise.

IBM.

HIMSS Healthcare Security Briefing

Michael R. Ash DDS, PMP, ITIL
IBM Healthcare Cybersecurity

6 April 2016
Polsinelli Conference Center, Kansas City

A bit about my background…

- Associate Partner at IBM in the Security, Strategy, Risk & Compliance sector
- Have 10 years of clinical experience as an oral surgeon working in hospitals
- Undergrad in computer science and electronic engineering with over 20 years in systems integration
- Worked at the Pentagon in healthcare informatics as a lieutenant colonel select
- Focused on healthcare cyber security, yet have worked all over the world for multiple corporations in a variety of fields

What we going to cover

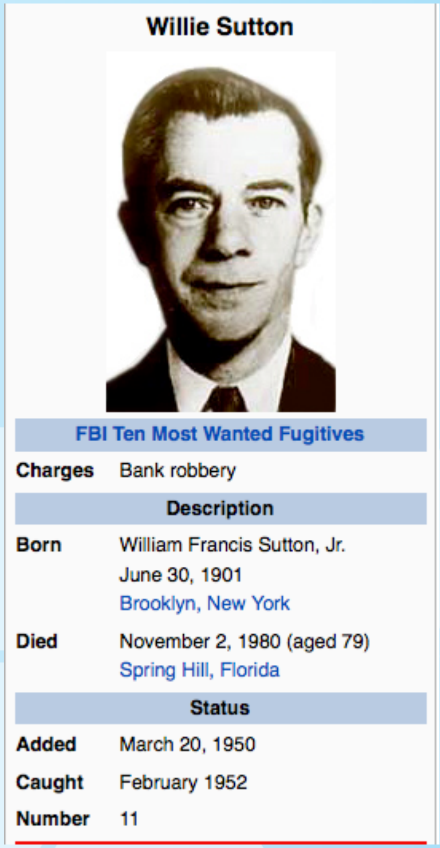
1. State of healthcare cybersecurity today
2. What are the risks
3. What you need to know with respect to mitigation
4. Discussion…

It’s where the money is….

When Willie Sutton was asked why he robs banks, he said: “I rob banks because that’s where the money Is…”

… this is the same reason that organized cybercriminals go after healthcare records... it’s where the money is.

Healthcare record lost or stolen in a breach could cost the victim organization as much as $363/record, fully 136% higher than the global average cost of a data breach per lost or stolen record.[1]



Willie Sutton

FBI Ten Most Wanted Fugitives	
Charges	Bank robbery
Description	
Born	William Francis Sutton, Jr. June 30, 1901 Brooklyn, New York
Died	November 2, 1980 (aged 79) Spring Hill, Florida
Status	
Added	March 20, 1950
Caught	February 1952
Number	11

[1] Ponemon Institute’s 2015 Cost of Data Breach Study / http://video.cnbc.com/gallery/?video=3000500545

Why is healthcare special…

- *Healthcare record compromise is up 1100%* this past year with over 100M records compromised. Considering there are 321M people in US means that 1:3 had healthcare records compromised in 2015
- *High value target*: Credit cards are worth about $3 where healthcare records worth $360
  - Includes SSAN, addresses past and present, contact information, insurance data, all immutable data meaning it's not easily changed
- *Loose federation* of systems with fine balance between usability and security
- *Security resources* are hard to find and retain
- *Multiple attack surfaces*:
  - Electronic Medical Record Systems (EMR)
  - 3rd party systems (payers, transcription, etc.)
  - Medical devices
  - Remote providers and contractors
  - Online patient access

Healthcare 411

You don't know what you don't know…

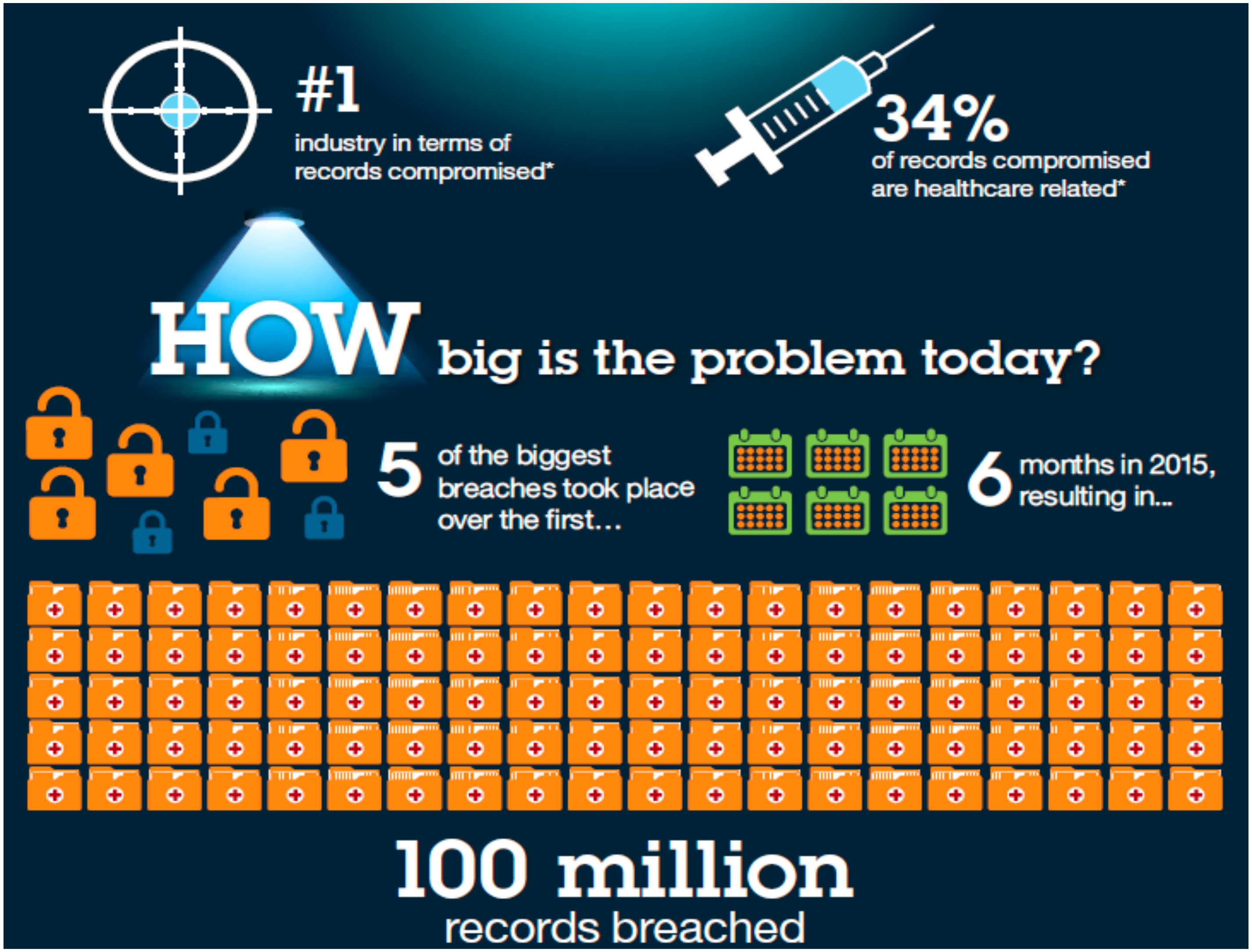
1. In addition to record lost, HIPPA fines can be as high as \$1.5M[2]
2. Hospitals have higher security exposure when compared to other industries considering the amount of PII and PHI[3] stored in multiple systems
3. Healthcare organizations as a culture not as security aware, managing risk without access to skilled security staff, many without C-level sponsorship
4. Some organizations have the perception is that it is cheaper to potentially pay fines instead of investing in security
5. Many healthcare delivery systems have no idea their medical devices are at risk[4]
6. Cybercrime is a significant threat to business, *world's largest illegal economies*, accounting for *$445 billion in annual profits* according to the United Nations.

1) 2015 Ponemon study: 2015 Cost of Data Breach Study: Global Analysis; 2) https://kb.iu.edu/d/ayzf; 3) Protected health information; 4) http://www.wired.com/2014/04/hospital-equipment-vulnerable/

Consider the following statistics…

- ✓ The rise of zero-day attacks and advanced evasion techniques have shifted the security landscape, changing the nature of network security
- ✓ According to IBM X-Force Data, 28% of overall vulnerability disclosures in 2015 were targeted at Web applications.
- ✓ At any given time, malicious code infects more than 11.6 million mobile devices. To put that figure into perspective, it's roughly equivalent to the population of Ohio. Hacking kits more powerful and less expensive
- ✓ The 2015 Ponemon Institute report, found that 50 percent of companies have zero budget dedicated to mobile app security, yet this is the fastest growing segment
- ✓ Between April 2014 and June 2015, the IC3 received 992 CryptoWall-related complaints, with victims reporting losses totaling over $18 million.

Healthcare data breaches: From sidelines to headlines


#1
industry in terms of records compromised*
34%
of records compromised are healthcare related*
HOW big is the problem today?
5 of the biggest breaches took place over the first…
6 months in 2015, resulting in…
100 million
records breached

Five of the eight largest healthcare security breaches over the last five years happened during the first six months of 2015.

Despite a quiet second half of the year, healthcare remains the leading industry in terms of records compromised

The cost of breaches are highest in healthcare

WHAT is the payoff for cyber criminals?

Prices on the black market are higher for health records than credit card numbers

WHY are health records so valuable?

Name
Address
Email address
Social security number
Date of birth
Insurance information
Employment
Medical history

With all the information in a health record, cyber criminals have many options:

- Steal your identity
- Use your insurance
- Launch targeted phishing attacks
- Destroy your reputation

Spear phishing, fraud and medical identity theft are just a few of the ways attackers can leverage electronic health record data.

Industry wide avg. cost / record

$154

Healthcare

$363

Pharmaceutical

$220

Attacks are focusing on higher value data targets

Driving demand for more integrated capabilities to thwart adversaries

2013

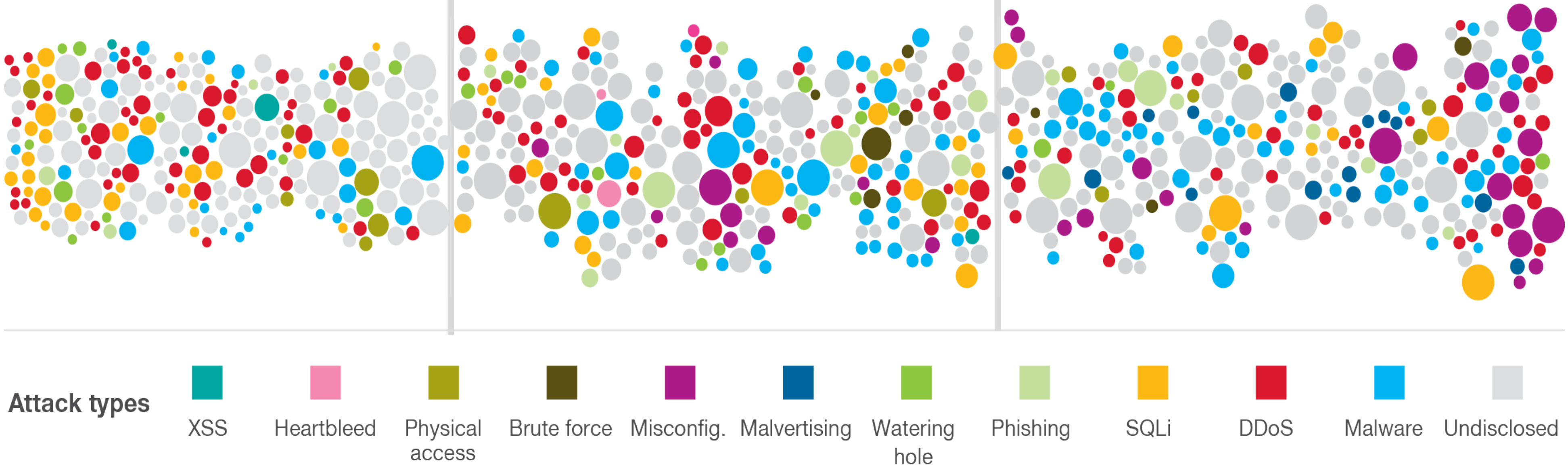
800,000,000+ records breached, with no signs of decreasing in the future

2014

1,000,000,000 records breached, while CISOs cite increasing risks from external threats

2015

Healthcare mega-breaches set the trend for high value targets of sensitive information



Source: IBM X-Force Threat Intelligence Report - 2016

Issues: Legacy systems and processes, lack of funding

- Migration to newer versions of an operating system or web browser requires time and money, and a lack of funding may be one of the fundamental obstacles
- Healthcare companies may still use legacy processes without updating security practices, i.e. keeping paper copies of records or not encrypting PHI

The ideal spend on security is

13.7%

of the overall IT budget[2]

Nearly half of healthcare organizations surveyed spend

3% or less

of their IT budgets on security[1]

[1] http://www.himss.org/News/NewsDetail.aspx?ItemNumber=28504

[2] http://www-03.ibm.com/industries/ca/en/healthcare/documents/IDC_Canada_Determining_How_Much_to_spend_on_Security_-_Canadian_Perspective_2015.pdf

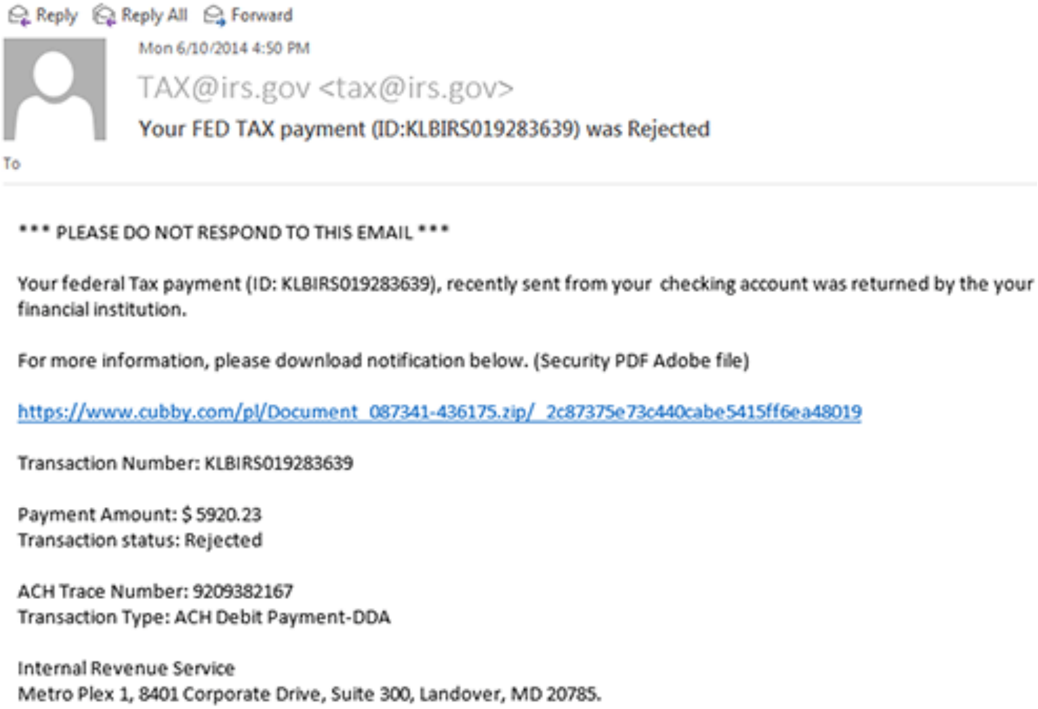
What are the threats you need to worry about..

- ***Internal Threats***
  - Either innocent or malicious acts that damage data, applications or systems
- ***External Threats***
  - The 40hr break even for Cybercriminal to take over your data
- ***Stolen credentials***
  - Use to steal money from facility or enable fraudulent insurance claim
- ***Phishing Attacks***
  - Perfectly formed eMails from FedEx for example, that contain link to malware site
- ***Ransomware***
  - Ransomware is malware that encrypts files and deletes the original files unless a ransom is paid, usually in untraceable bitcoin.
    - Cyber crime profits over $1B In a recent survey, 30 percent of security professionals were willing to negotiate. Among organizations already victimized by cybercriminals the figure rose to 55 percent.

Ransomware…. How do they get in?

- Email / Social Engineering
  - Attachment (DOC, PDF, ZIP, CAB, etc.)
  - Link to a booby-trapped website
  - Phishing eMails
- Drive-by-Download
  - Malvertising
  - Compromised web-sites
  - Links in social networking posts (FaceBook, Twitter, etc.)
- Previously Compromised/Infected System
  - System already infected
  - Usually with a bot client (malware)
- *Unpatched systems (a common target)*

Recent survey carried out by the University of Kent found that 41% hit by ransomware, paid the ransom…



Mon 6/10/2014 4:50 PM

TAX@irs.gov <tax@irs.gov>

Your FED TAX payment (ID:KLBIRS019283639) was Rejected

*** PLEASE DO NOT RESPOND TO THIS EMAIL ***

Your federal Tax payment (ID: KLBIRS019283639), recently sent from your checking account was returned by the your financial institution.

For more information, please download notification below. (Security PDF Adobe file)

https://www.cubby.com/pl/Document_087341-436175.zip/_2c87375e73c440cabe5415ff6ea48019

Transaction Number: KLBIRS019283639

Payment Amount: $ 5920.23
Transaction status: Rejected

ACH Trace Number: 9209382167
Transaction Type: ACH Debit Payment-DDA

Internal Revenue Service
Metro Plex 1, 8401 Corporate Drive, Suite 300, Landover, MD 20785.

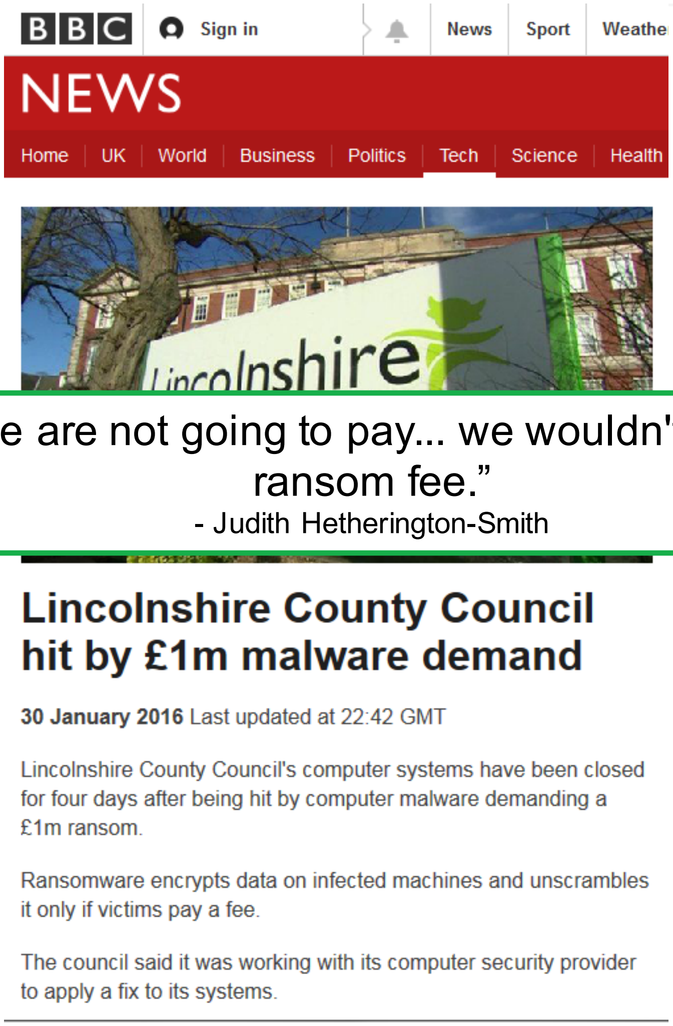
Ransomware Process

- ***Infection***
  - Via social engineering, phishing, weakness in unpatched versions of Office, Flash, or PDFs, and infrastructure attacks; webserver are the most common targets

- ***Execution***
  - Encrypts files then provides instructions to pay for decryption key.
  - You don't have to lock an entire network, just the critical files in a network
  - *Recent targets:* MedStar Health forced to turn patients away after Ransomware attack. Others include Sacred Heart Health System, Hollywood Presbyterian, Titus Regional Medical Center, Valley Hospital, Ridgewood, Englewood Hospital, Holy Name Medical Center and Kentucky Methodist. *Locky a common variant*. SamSam attacks webservers vulnerabilities in ***JBoss apps using an open source pen testing tool called JexBoss***

- ***The Payoff***
  - CryptoLocker strain of ransomware stole some $27 million in just six months out of people whose data they took hostage.

Ransomware Decision



Lincolnshire County Council hit by £1m malware demand

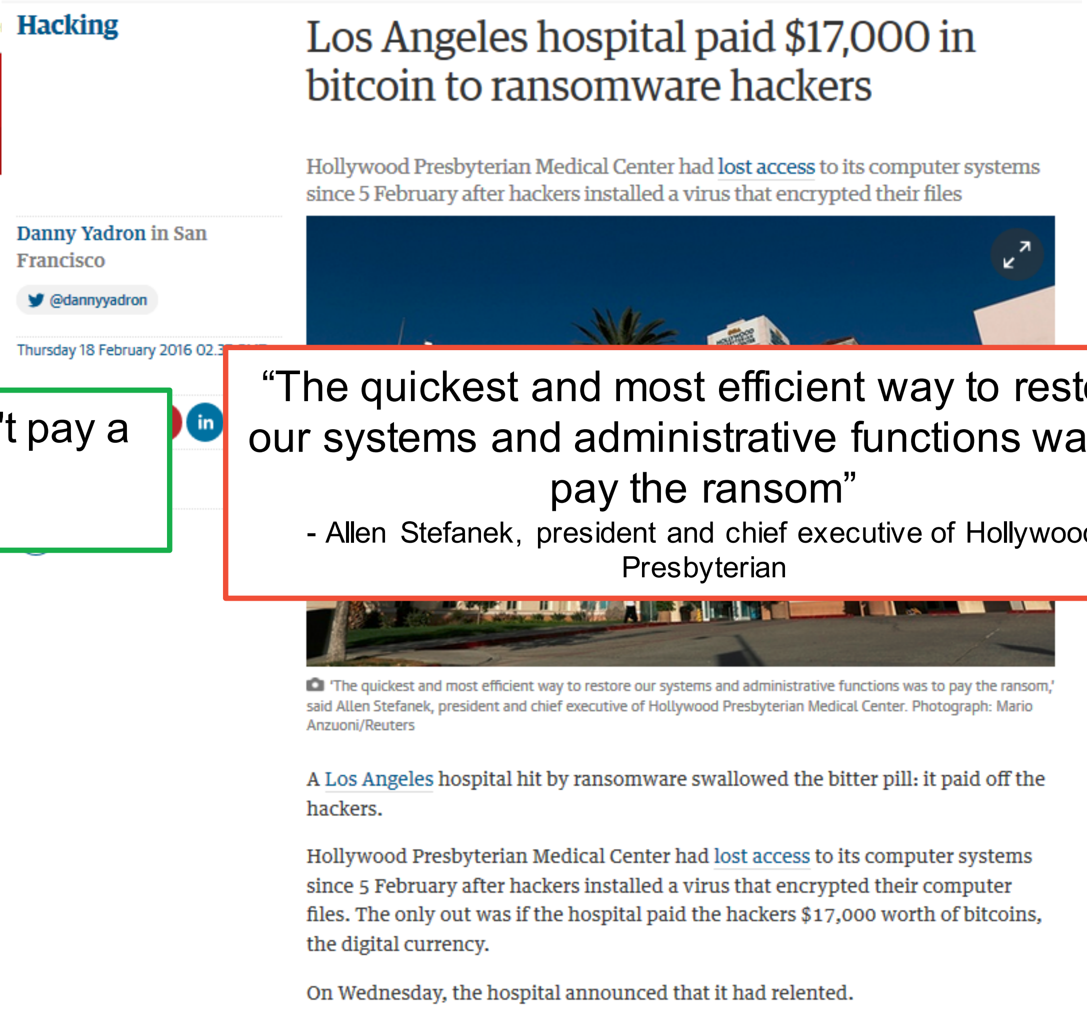
30 January 2016 Last updated at 22:42 GMT

Lincolnshire County Council's computer systems have been closed for four days after being hit by computer malware demanding a £1m ransom.

Ransomware encrypts data on infected machines and unscrambles it only if victims pay a fee.

The council said it was working with its computer security provider to apply a fix to its systems.

"We are not going to pay... we wouldn't pay a ransom fee."
- Judith Hetherington-Smith



Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

Danny Yadron in San Francisco

@dannyyadron

Thursday 18 February 2016 02.3

'The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom,' said Allen Stefanek, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni/Reuters

A Los Angeles hospital hit by ransomware swallowed the bitter pill: it paid off the hackers.

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their computer files. The only out was if the hospital paid the hackers $17,000 worth of bitcoins, the digital currency.

On Wednesday, the hospital announced that it had relented.

"The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom"
- Allen Stefanek, president and chief executive of Hollywood Presbyterian

Ransomware Mitigation

1. Ensure that your endpoints and servers are ***patched*** and up-to-date with appropriate endpoint protection implement.
2. ***Train*** and test staff on safe email and Web-browsing practices, and periodically test their behavior. (http://phishme.com/)
3. Confirm strong email ***filtering***
4. Confirm strong and enforceable group ***policy*** for Active Directory users that restrict permissions to prevent propagation of malware
5. Test to see if servers up to date for OS and application ***patches***
6. Verify that ***firewall*** rules are well written
7. Use multiple up to date ***Antivirus*** products
8. Verify a strong and tested ***backup*** policies. Key is to keep backups near online so that they are not accessible by the hacker but quick to bring back online.
9. Confirm networks are architected to provide ***segmentation*** thereby preventing hackers from moving across network to other systems.

Ransomware… What can you do now?

1. If you have J-Boss webserver know there is vulnerable to SamSam Cryptoware *(it doesn't need phishing or drive-by web link)*
2. Double check your patch management plan to make sure systems current
3. User education on phishing attacks
4. Get a vulnerability assessment <$50K – depending on number of endpoints
5. Make sure your network is segmented so attacker can spread malware
6. If attacked, shut down networks including WiFi to prevent spread and have user remove USB sticks and any connected drives.
7. Get an Emergency Response Team engage early to minimize damage

Find out what you don’t know…

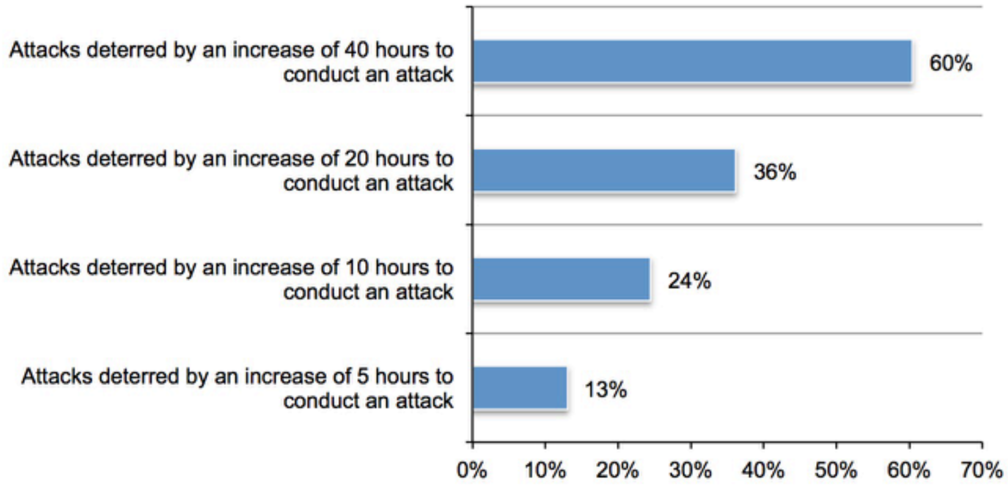
Two type of hospitals, those that have been hacked and those that don’t know it yet…

- ***Current status***
  - Complex environment with unknown security risk
  - Limited budget drives the need for prioritized roadmap
  - Limited access to specialized security staff
- ***What’s needed***
  - Make sure you have current security audit
  - Use a risk tools to match control status against historic events
  - Look beyond controls by mapping again potential threats
  - Do an external vulnerability assessment
  - Know who your Emergency Reponses Provider is…
  - Practice disaster recovery process

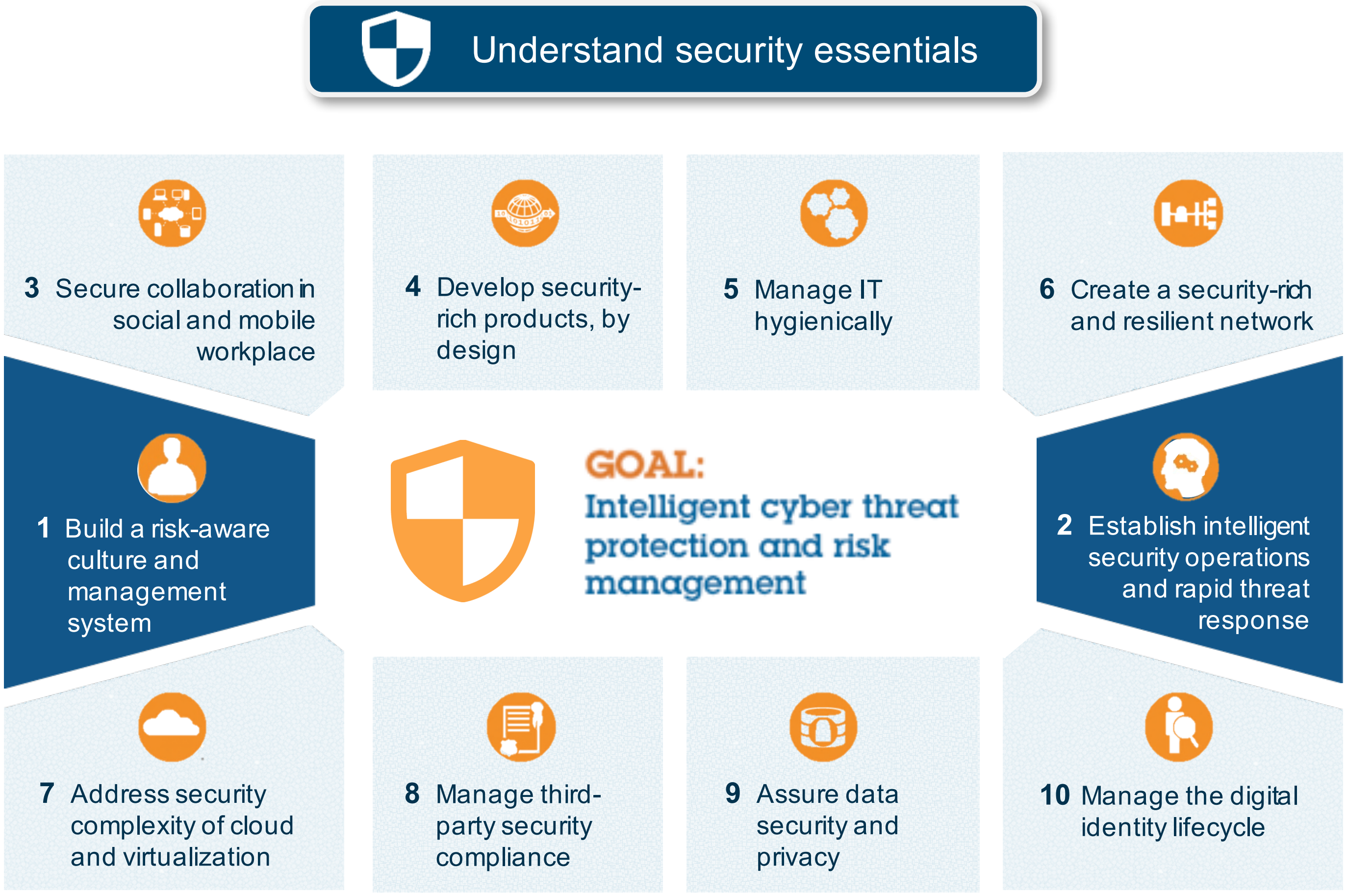
Don’t be the ”soft target”

- *Cybercrime is now the #1 paying criminal activity over drugs, trafficking, and extortion - The Russian Mafia, which successfully stole $9 million dollars this way in 2008*
- *From:* Ponemon Study: Crime Can Pay Hackers Flipping the Economics of Cyber Attacks – the key is to be more secure than others in your industry – *Forty hours seems to be the ROI*

Figure 8. When will a hacker call it quits?
Consolidated view



Review all elements of people, process, and technology



Understand security essentials

3 Secure collaboration in social and mobile workplace

4 Develop security-rich products, by design

5 Manage IT hygienically

6 Create a security-rich and resilient network

1 Build a risk-aware culture and management system

GOAL:
Intelligent cyber threat protection and risk management

2 Establish intelligent security operations and rapid threat response

7 Address security complexity of cloud and virtualization

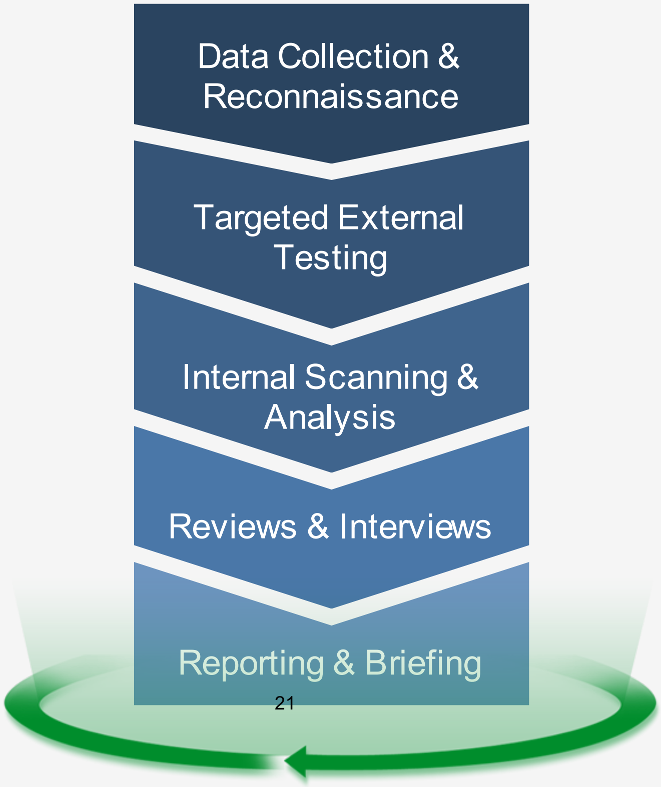
8 Manage third-party security compliance

9 Assure data security and privacy

10 Manage the digital identity lifecycle

Perform an Active Threat Assessment (ATA)

Uncover indicators of compromise and hidden threats


Data Collection & Reconnaissance
Targeted External Testing
Internal Scanning & Analysis
Reviews & Interviews
Reporting & Briefing
21

- **Coordinated Attack Simulation**
  Targeted penetration testing helps identify vulnerable systems and applications from an attacker's perspective, conducted with broad coverage or using a customized and simulated events. An on-site coordinator assists with validating that detection mechanisms are successfully detecting malicious activity.

- **Tool based APT Forensic Scanning**
  Checks for the presence of behavioral Indicators of Compromise (IOCs) frequently seen with intrusions indicating a currently active but previously unknown compromise.

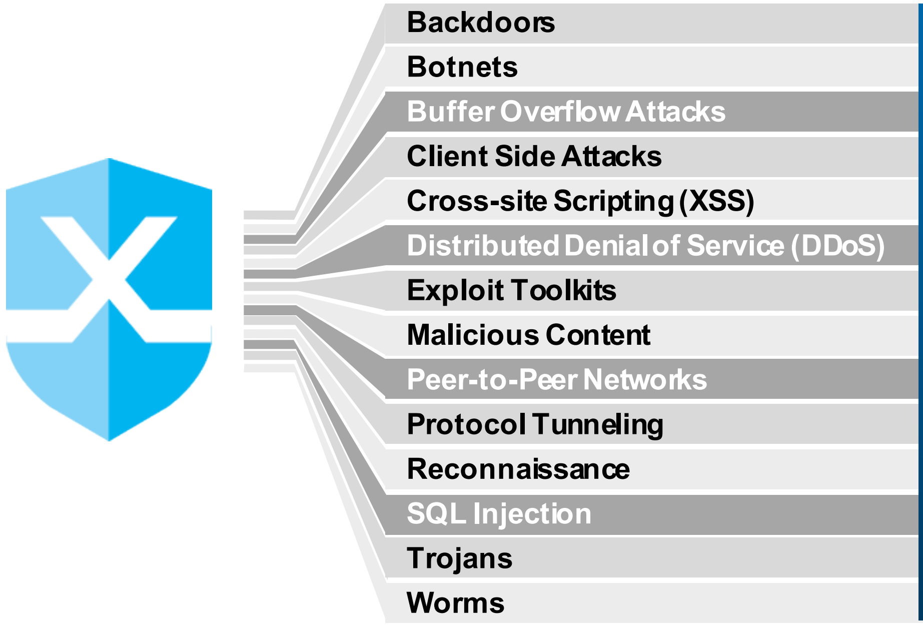
- **Memory (RAM) Analysis**
  For systems identified with suspicious activity, a remote memory (RAM, volatile data) analysis may be done looking for common malware traits.

- **System Log Analysis**
  Logs from firewalls, IDS/IPS devices, Network AV servers, DNS and other systems can help reveal IOCs of an intruder or the presence of malware.

- **Critical Controls Review**
  Assessment of the level of implementation of SANS Top 20 Critical
  Security Controls helps to develop an overall security strategy.

X-Force® Research and Dynamic Threat Intelligence

Expert analysis and data sharing on the global threat landscape



- Backdoors
- Botnets
- Buffer Overflow Attacks
- Client Side Attacks
- Cross-site Scripting (XSS)
- Distributed Denial of Service (DDoS)
- Exploit Toolkits
- Malicious Content
- Peer-to-Peer Networks
- Protocol Tunneling
- Reconnaissance
- SQL Injection
- Trojans
- Worms

Sharing real-time and anonymized threat intelligence

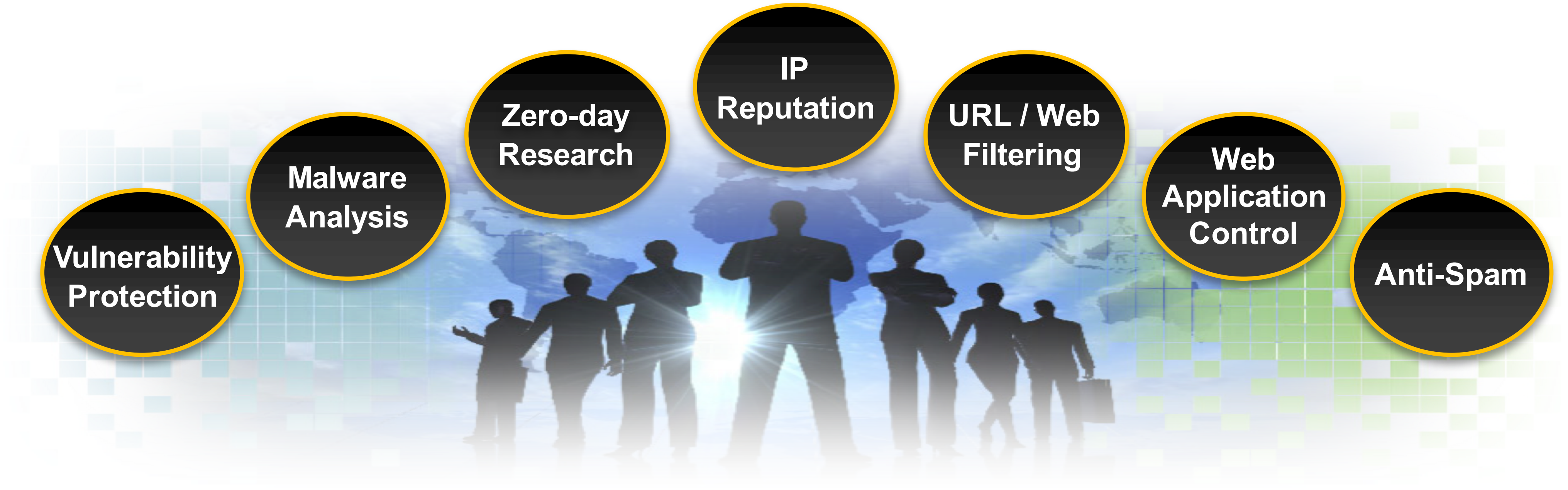
Security Operations Centers

X-Force Helps Keep Customers Ahead of the Threat

- Cataloging, analyzing and researching vulnerabilities since 1997
- Providing zero-day threat alerts and exploit triage to customers worldwide
- Building threat intelligence from collaborative data sharing across thousands of clients
- Analyzing malware and fraud activity from 270M+ protected endpoints

X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape



The X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

IBM X-Force monitors and analyzes the changing threat landscape

Coverage

20,000+ devices under contract

15B+ events managed per day

133 monitored countries (MSS)

3,000+ security related patents

270M+ endpoints reporting malware

Depth

25B+ analyzed web pages and images

12M+ spam and phishing attacks daily

89K+ documented vulnerabilities

860K+ malicious IP addresses

Millions of unique malware samples

Leverage free resources…

- IBM Security Intelligence Blog – http://securityintelligence.com/
- IBM X-Force Exchange Community – https://exchange.xforce.ibmcloud.com/
- Google: ibm x-force exchange and click on "Try the Platform"… it's free!
  - https://exchange.xforce.ibmcloud.com/

- You'll know you're a the right place if you don't get an image like this…

IBM can make the difference… .

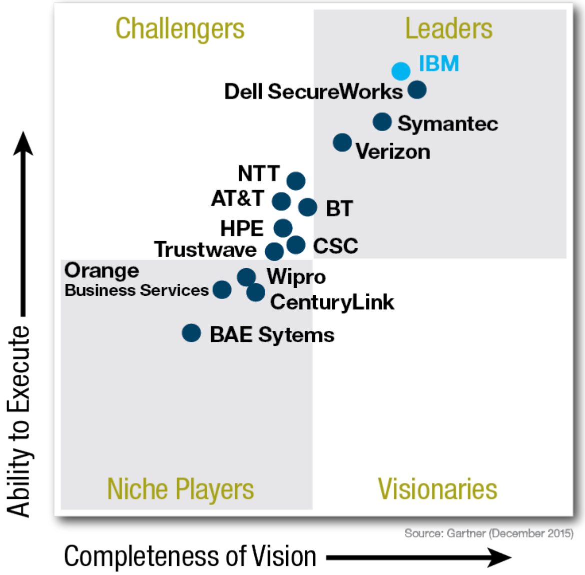
- The Leader 13 out of 15 of Gartner segments, nearest competitor has less than 5.
- Top reviews from Forrester and IDC.
- The industry's first integrated end-to-end Security Operations and Response Platform that will span the entire lifecycle of a cyber attack
- The only vendor with a comprehensive best of breed integrated software and services offerings with over 5000 security professionals.
  - If you take out antivirus companies, IBM is the the largest enterprise security vendor in the market
- Global reach with data from 133 monitored countries with over 270M endpoints reporting malware while analyzing over 15B events per day
- Can provide you with unparalleled security analysis, recommendations, and services.

IBM Security Services is built upon a track record of delivering results

Recognized by major analyst firms for our global capability and ability to execute

Gartner

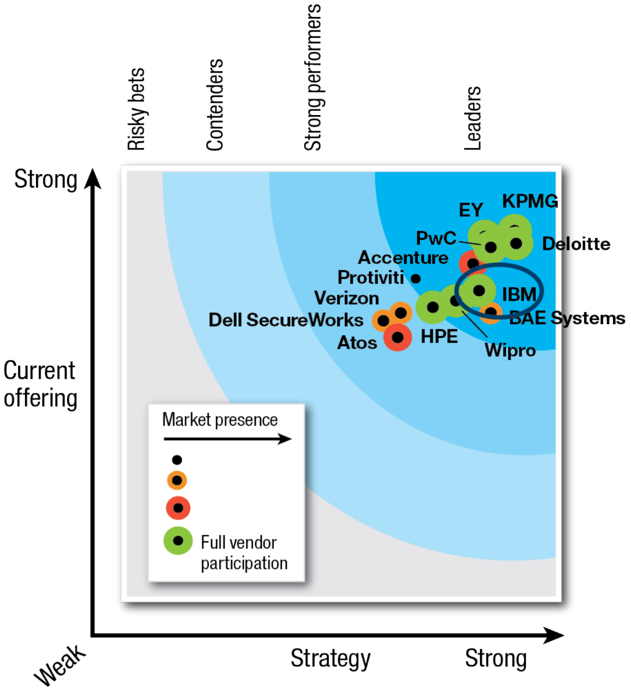
Magic Quadrant for Managed Security Services, Worldwide



Source: Gartner (December 2015)

FORRESTER

Wave for Information Security Consulting Services



Gartner

Named **Leader** in Managed Security Services (2015)

FORRESTER

- Named **Leader** in Security Consulting (2015)
- Named **Leader** in Managed Security Services (2014)

FROST & SULLIVAN

Named **Leader in** Managed Security Services (2015)

IDC Analyze the Future

Named **Leader in** Managed Security Services (2014)

Current Analysis.

Named **Leader** in Managed Security Services (2014)

What differentiates IBM Security?

Our ability to offer clients solutions and results.

Intelligence and analytics.

Advanced analytics to protect against cybercrime.

25 security labs deliver security breakthroughs.

An integrated approach.

Integrated portfolio of security **services and technology**.

Open ecosystem with 100+ technology partners.

Unparalleled expertise.

Unmatched **security practices** from thousands of engagements.

35 billion security events managed per day.

IBM Security Quals

IBM **Security**

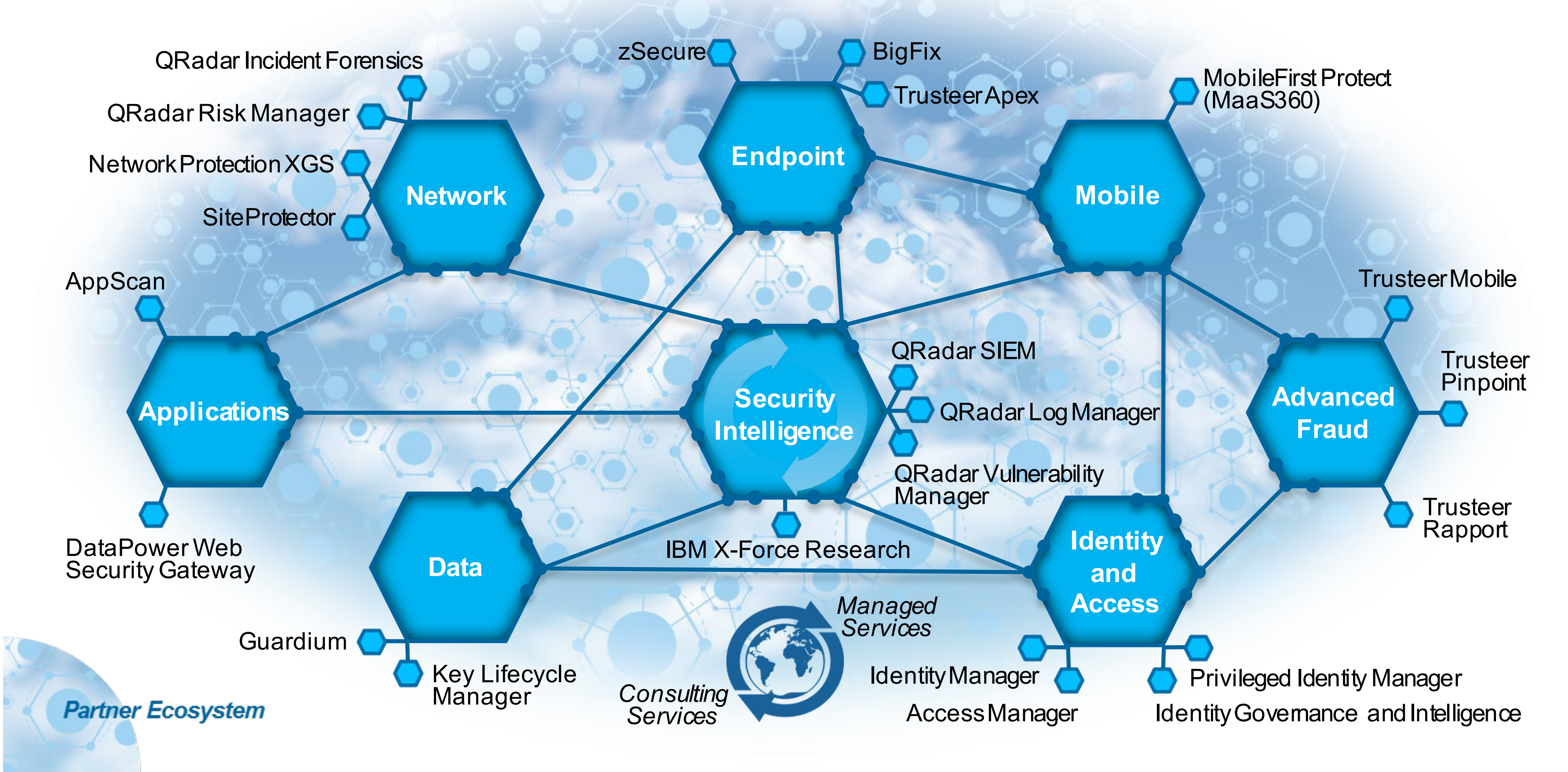
Intelligence. Integration. Expertise.

TOP 2	enterprise security software vendor in total revenue. #1 if you take out antivirus companies
24	industry analyst reports rank IBM Security as a **LEADER**
133	countries where IBM delivers managed security services
12K	clients protected *including…*
22	of the top 29 banks in Japan, North America, and Europe

V2015-07-29

Expand the value of security solutions through integration

Continuous actionable intelligence



Discussion…

Michael R. Ash DDS, PMP, ITIL
mash@us.ibm.com
(760) 330-7639

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM **Security**

Intelligence. Integration. Expertise.

Legal notices and disclaimers

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml