Ingredients of a Holistic Approach to Information Security Risk Management

Presented by

Gerry Blass, ComplyAssistant and Mike Chirico, Sensato

HIMSS NEW JERSEY Chapter

TRANSFORMING HEALTHCARE THROUGH IT

Agenda

- Background Information
- Breaches and Incidents
- Holistic Approach
- CyberSecurity
- Summing it Up

- **Gerry Blass**
- **President & CEO of ComplyAssistant**
- Gerry Blass brings over 30 years of experience in healthcare information technology. Prior to ComplyAssistant, Gerry was the Chief Information Security Officer (CISO) for a major healthcare system in New Jersey.
- In 2002 Gerry founded ComplyAssistant to provide software and service solutions for HIPAA and IT strategic planning. Today, ComplyAssistant provides software and service solutions to over 100 healthcare organizations with a focus on compliance regulations, including HIPAA-HITECH-OMNIBUS, PCI, HITRUST, Meaningful Use, Accreditation, OIG (federal and state), Conflict of Interest, and other federal and state healthcare regulations.
- Gerry is an active member of HIMSS and participates in national and various chapter events. Gerry contributes to industry publications and actively shares content in HIPAA 411, a LinkedIn group he co- founded, along with many other related LinkedIn groups. Gerry presents at industry association events, including HIMSS, HFMA, AITP, NCHICA, and HCCA. Gerry was recently elected to the New Jersey HIMSS Board of Directors, and heads up the Security, Privacy and Compliance Task Force.

Mike Chirico Bio and Pic

Mike, a privacy and security attorney, has over twenty years of experience with various public accounting firms, including several Big Four firms, providing a broad range of advisory services including IT General Control audits, business process redesign and improvements, internal audit co-sourcing, pre & post implementation reviews, business continuity and disaster recovery, Sox 404 Compliance, and Service Organization Control Reporting. Mike is also an attorney in New Jersey.

- Additional experience includes: documentation, controls rationalization, compliance testing and reporting; extensive experience evaluating, designing and managing IT audit methodologies; Performed Service Organization Control testing & reporting (SOC One & Two). Mike has assisted many clients with evaluating and re-engineering IT policy & procedure taxonomy to satisfy regulatory scrutiny.

holistic

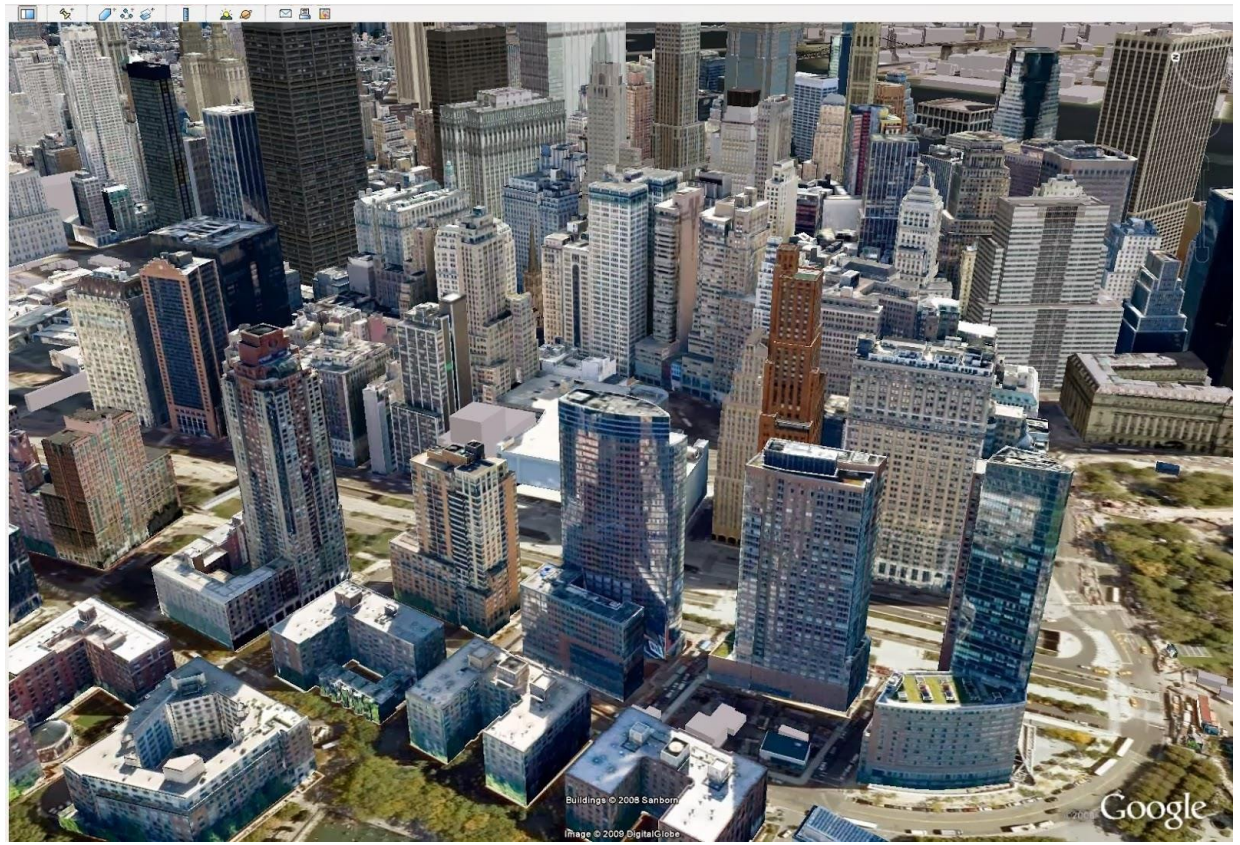
Holistic means encompassing the whole of a thing, and not just the part. *Holistic* medicine looks at the whole person for answers, not just at physical symptoms.


SALES
RESEARCH
CUSTOMER
PLAN
ANALYSIS
PLANNING
IMPLEMENTATION
COMPLEX
ASSESSMENT
IMPACT
MONITOR
MANAGEMENT
ORGANIZATION
DATA
IDENTIFICATION
RISK
OPPORTUNITY
PROCESS
COST
MANAGEMENT
EVALUATION
SCOPE
TREATMENT
STRATEGY
PLAN
EVALUATION
RESOURCES
SOLUTION
IMPORTANT
RISK

Background Information

Seems easy from 30,000 Feet

And more complicated up close!



Observations

- Lack of organizational mandates and oversight
- Political obstacles
- Lack of adequate $$ and human resources to mitigate risk
- Policies for the most part were not fully operational and evidence documentation is not organized or does not exist

Results

- Increased data breaches
- Government audits were no longer reactive, but also proactive
- HITECH (2009)
- Omnibus (2013)
- Increased penalties and lawsuits for both CEs and BAs
- Orange is the new black

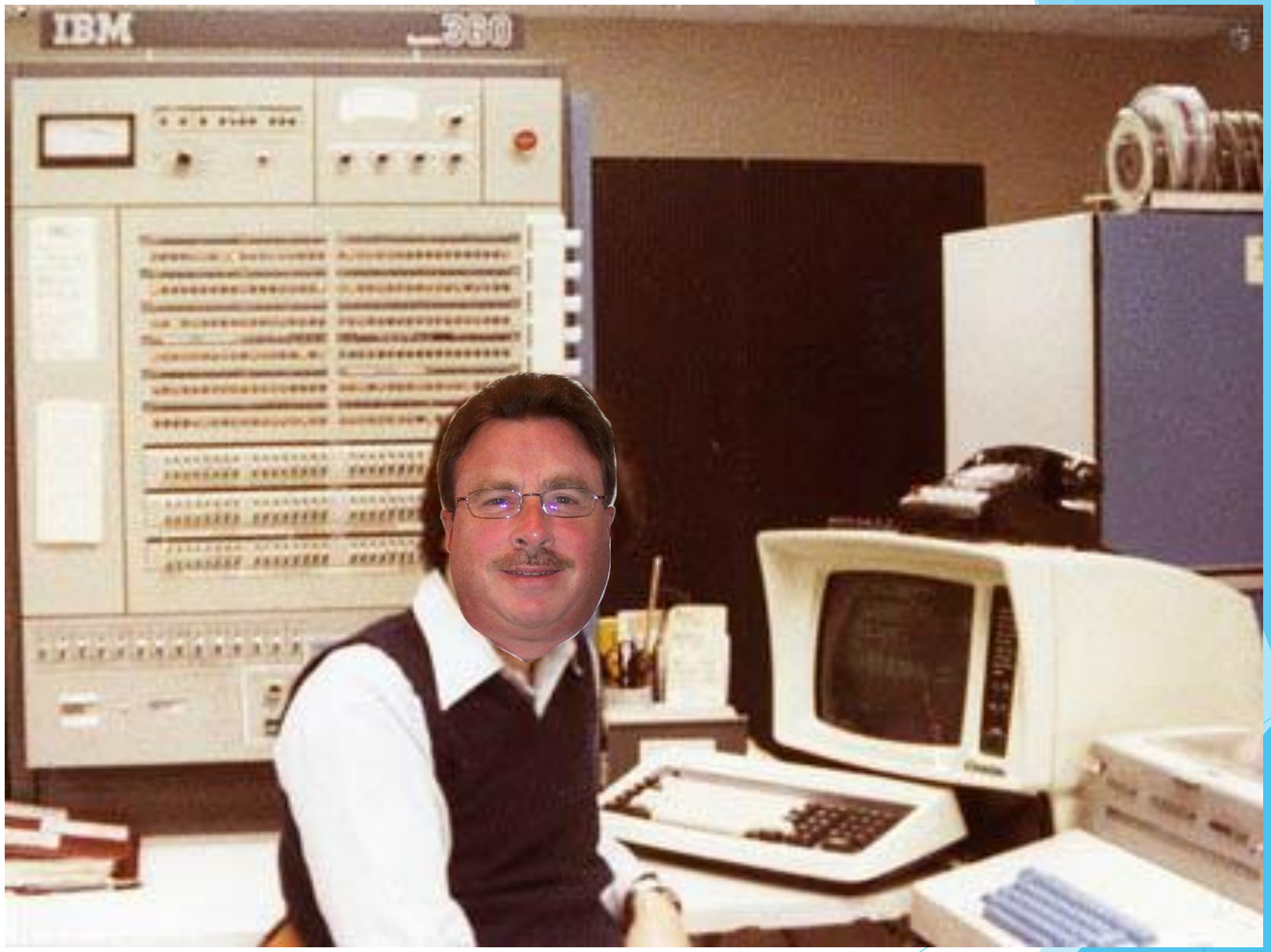
To know where we are and where we are going….

We need to look at where we have been…Yogi Berra?

Evolution – 1970s & 80s

Evolution - 1970s & 80s

Who is this?



Evolution - 1970s & 80s

Evolution – 1970s & 80s

Low Access – High Security:

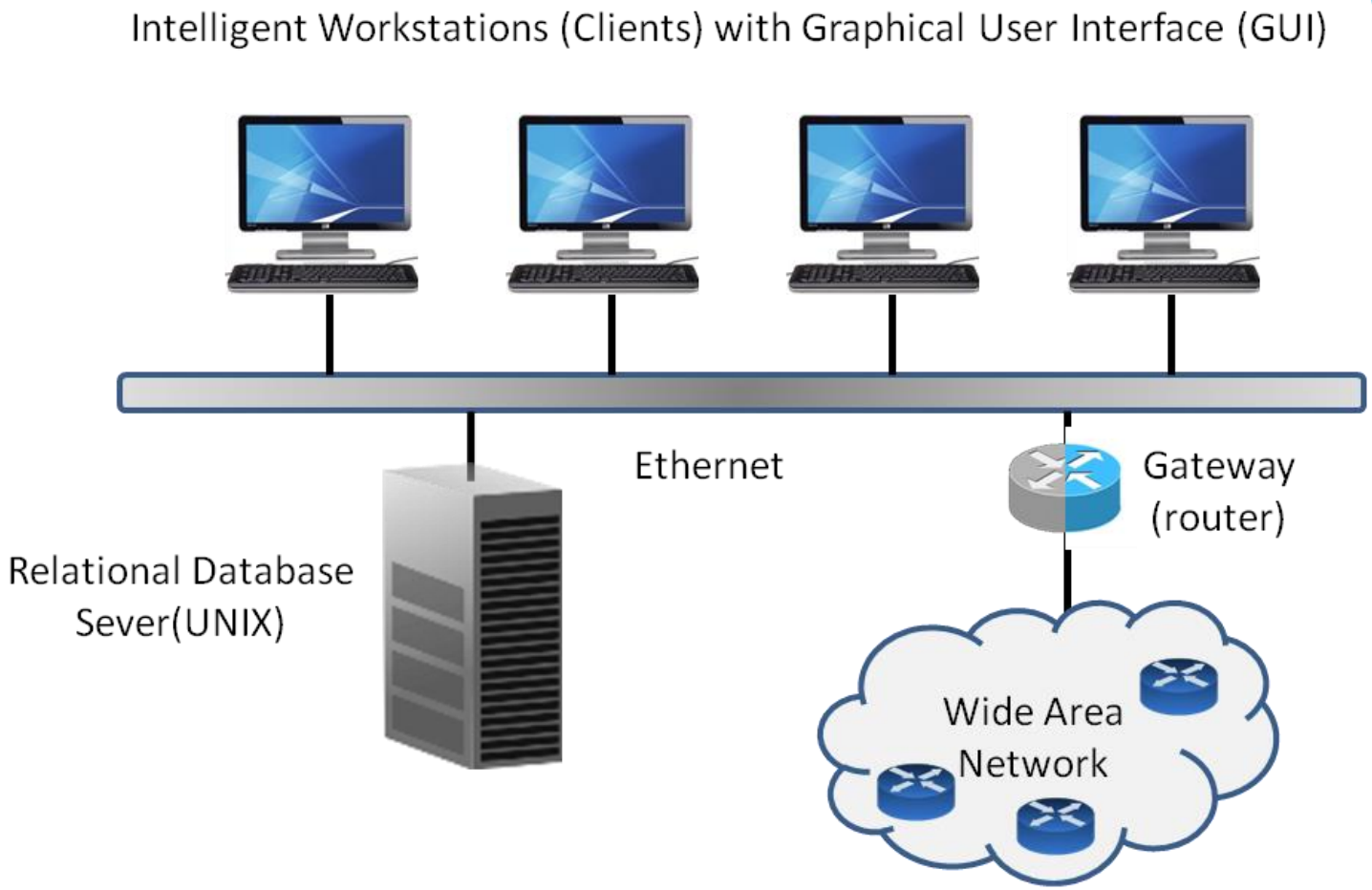
- Identifiable health information mainly in 3 places - on a main frame computer located in a secure computer room, on back up tapes at an offsite location, and on hard copy
- User workstations were “dumb”
- Access to information was limited
- Potential risk was much lower – mainly hard copy charts, reports and screen prints

Evolution - 1970s & 80s

Low Access – High Security:

- Motivation for unauthorized access for monetary gain was low
- Most unauthorized access was due to workforce concern for fellow employees, neighbors, etc..

Evolution - 1990s



Evolution - 1990s

Evolution – 1990s

The PC and Internet Storm:

- A numbers game
- Identifiable information in many places, unprotected
  - Lans and wans
  - Distributed servers
  - Smart workstations
  - Email
  - CDs

$$ Motivation

With reluctance, Arthur Ashe says he has AIDS Tennis pioneer criticizes tip to press that forced revelation.

April 09, 1992 | By Susan Reimer | Susan Reimer,Staff Writer

Arthur Ashe, a pioneering black man in professional tennis and an eloquent activist in issues of race and sports, said yesterday that he has AIDS.

"I have AIDS," he said. "I am sorry that I have been forced to make this revelation now, at this time."

Evolution – 1990s

The PC and Internet Storm:

- Arthur Ashe's PHI disclosed to the Enquirer
- Motivation increased for unauthorized access for monetary gain
- HIPAA signed into law in 1996
- By then, the technology storm made access to PHI easier which was good for providing care, but bad for information security

Breaches

- The "Hurricane of Technology” during the 1990s created geometric numbers of locations of PHI that have certainly contributed to the large number of breaches today

Evolution - The 2000's

Evolution - The 2000's

Evolution - The 2000's

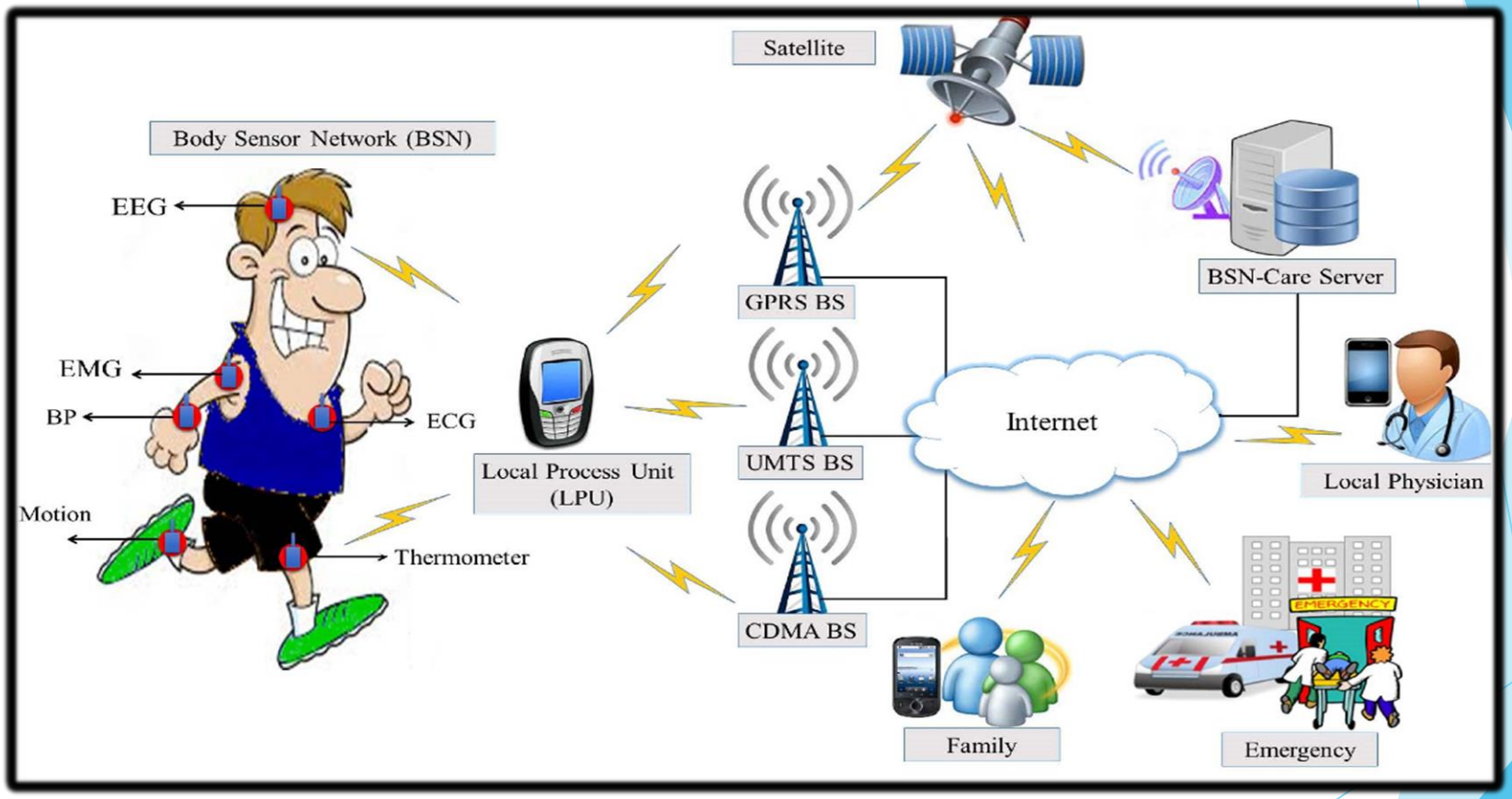
Evolution - The 2000's

Evolution - The 2000's

Evolution – The 2000's

Population Health Drives IoT

Service Delivery via the Internet of Things

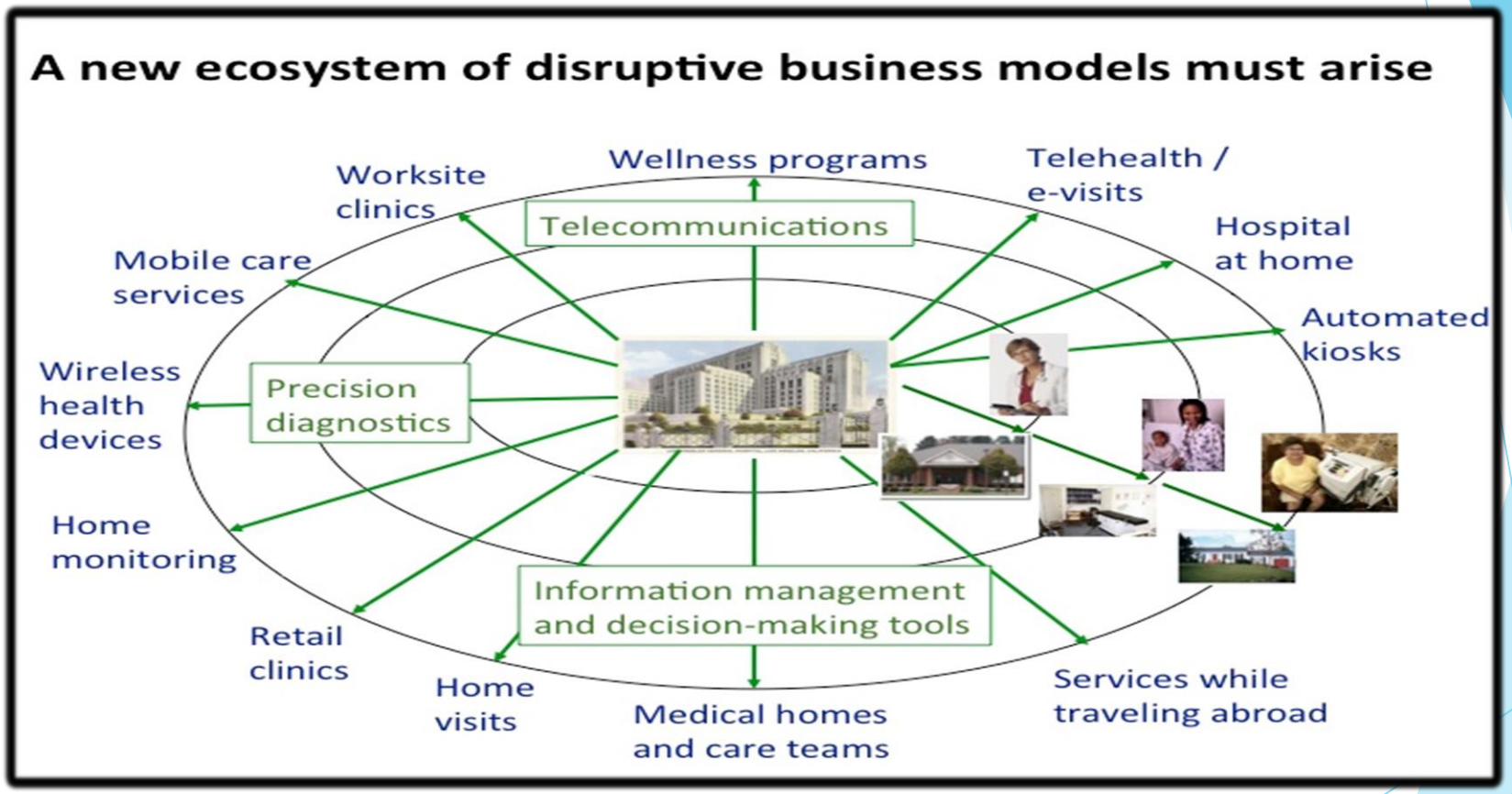


•Source: Semantic Scholar - BSN-Care

Evolution – The 2000's

Population Health - Disruption

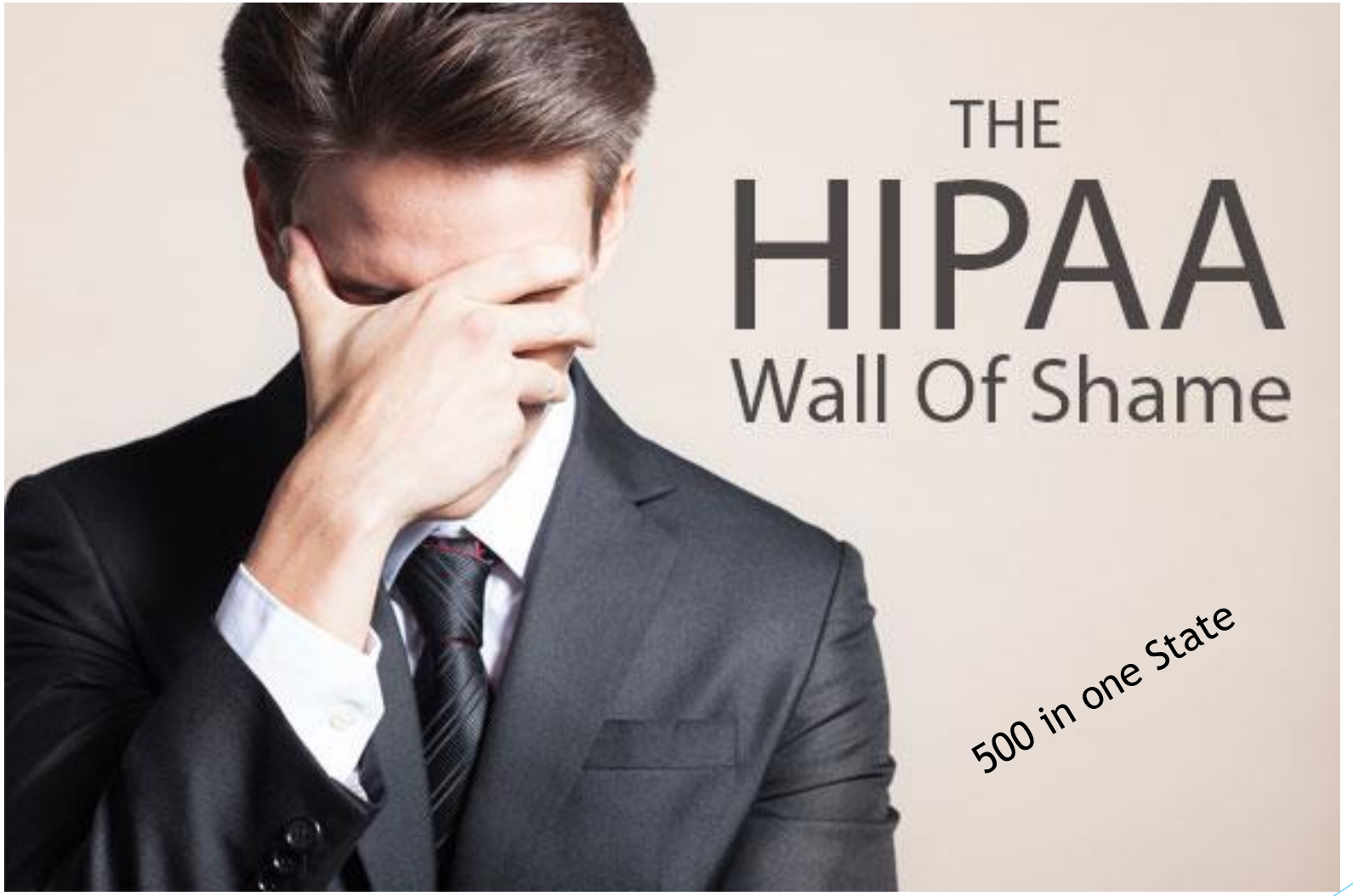
Starship Enterprise Security Scanner



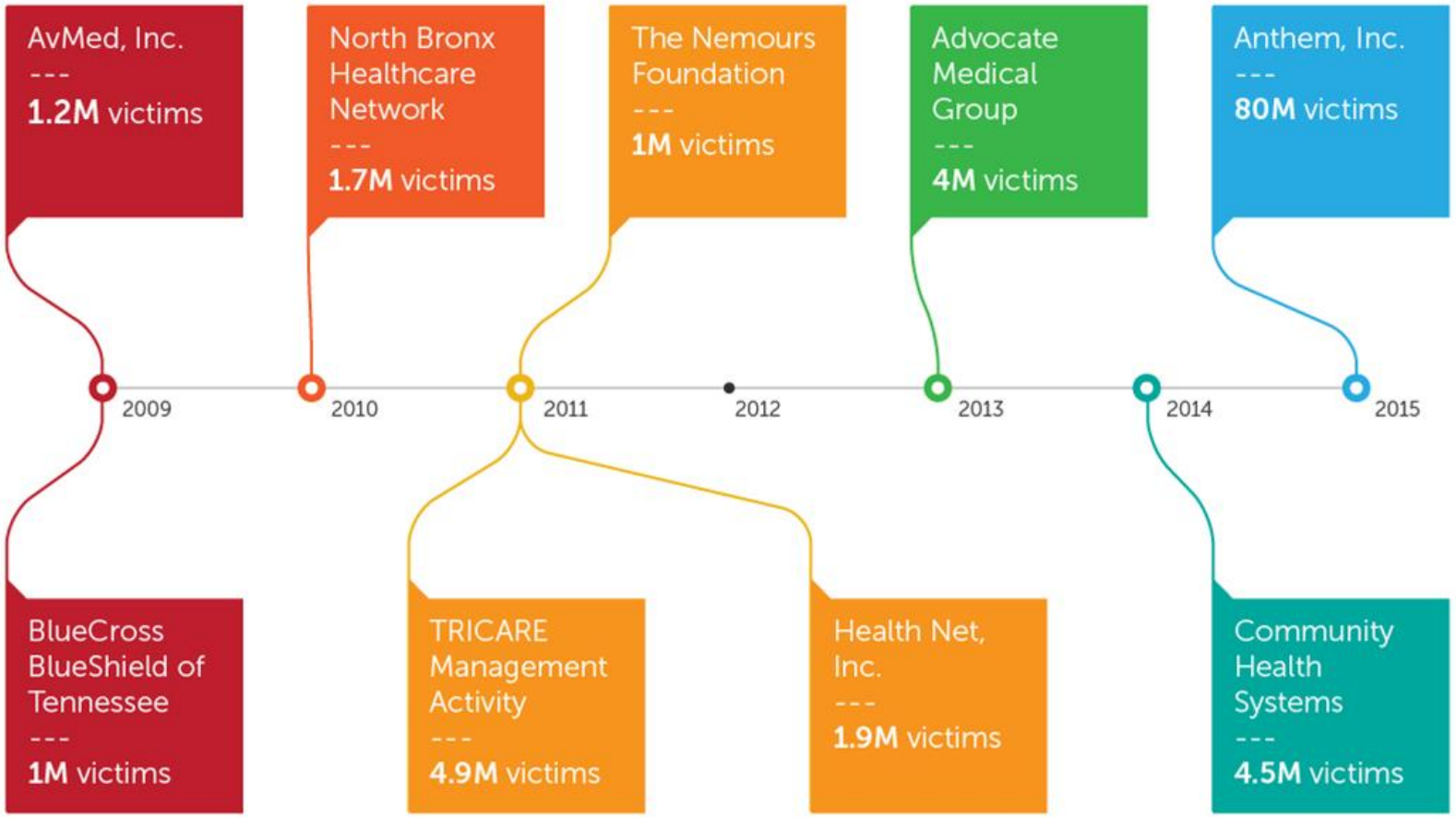
•Source: mnhospitals.org

Breaches / Incidents

- Since 2009, there has been a large increase with healthcare organizations migrating from hard copy to electronic medical records
- Much of it was done with a major focus on meeting Meaningful Use measures for $$ incentives
- The secondary focus in many organizations, especially smaller ones, was on information security
- In some cases a simple checklist was completed to be able to check the box on the measure that required an SRA
- As a result, the attackers considered healthcare to be a prime target


THE
HIPAA
Wall Of Shame
500 in one State

NOTABLE HEALTHCARE BREACHES



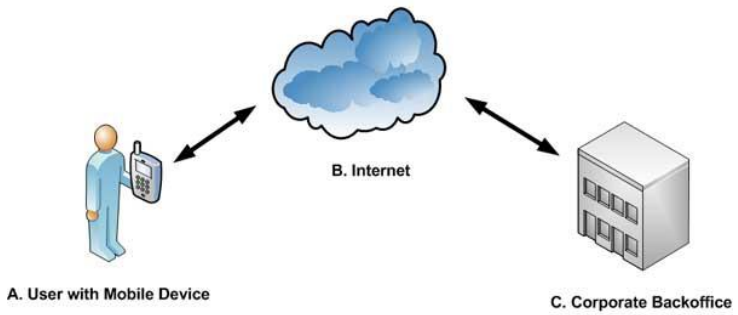
June 2017 - "We have no indication that customer data has been lost or removed from our network. We have made rapid progress in restoring our systems safely with enhanced security. As computers and systems are brought back online, we are adding further security controls as we work to restore full functionality for our customers".

140 million plus records breached!!

Admin, Admin !!

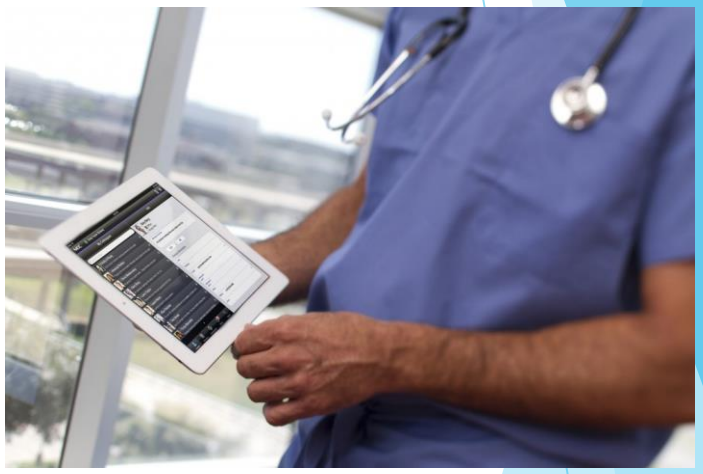
Holistic Approach

WHERE IS YOUR PHI?



Data in transit

Data at rest



Data in use

Need to protect against threats!

ELEMENTS OF AN HOLISTIC APPROACH

- Security Risk Assessments (SRAs)
  - **Rule Assessment**
  - Administrative Audits / Exercises
    - **PHI locations and controls**
    - Threat assessment
    - Policies and procedures
    - Proactive Recurring Audits
      - E.g. Employee and Third Party Vendor (BA) termination notifications
      - Facilities
    - Third Party Vendors (BAs) SRAs
      - Medical Device Vendors
      - Other MEDIUM to HIGH RISK BAs
  - Technical Testing and controls
  - Exercises
    - Disaster Recovery and Business Continuity
    - Cybersecurity

Rule Assessment

Part 164 - Security and Privacy
164 - Subpart C - Security Standards for the Protection of Electronic Protected Health Information
164.308 - Administrative safeguards.
164.308(a)(1)(i) - Security Management Process
164.308(a)(1)(ii)(A) - Risk Analysis (Required)
164.308(a)(1)(ii)(B) - Risk Management (Required)
164.308(a)(1)(ii)(C) - Sanction Policy (Required)
164.308(a)(1)(ii)(D) - Information System Activity Review (Required)
164.308(a)(2) - Assigned security responsibility.
164.308(a)(3)(i) - Workforce security
164.308(a)(3)(ii)(A) - Authorization and/or supervision(Addressable)
164.308(a)(3)(ii)(B) - Workforce clearance procedure (Addressable)
164.308(a)(3)(ii)(C) - Termination procedures (Addressable)
164.308(a)(4)(i) - Information access management.
164.308(a)(4)(ii)(A) - Isolating health care clearinghouse functions (Required)
164.308(a)(4)(ii)(B) - Access authorization (Addressable)
164.308(a)(4)(ii)(C) - Access establishment and modification (Addressable)
164.308(a)(5)(i) - Security awareness and training.
164.308(a)(5)(ii)(A) - Security reminders (Addressable)
164.308(a)(5)(ii)(B) - Protection from malicious software (Addressable)
164.308(a)(5)(ii)(C) - Log-in monitoring (Addressable)
164.308(a)(5)(ii)(D) - Password management (Addressable)
164.308(a)(6)(i) - Security incident procedures.
164.308(a)(6)(ii) - Response and Reporting (Required)
164.308(a)(7)(i) - Contingency plan.
164.308(a)(7)(ii)(A) - Data backup plan (Required)
164.308(a)(7)(ii)(B) - Disaster recovery plan (Required)
164.308(a)(7)(ii)(C) - Emergency mode operation plan (Required)
164.308(a)(7)(ii)(D) - Testing and revision procedures (Addressable)
164.308(a)(7)(ii)(E) - Applications and data criticality analysis (Addressable)
164.308(a)(8) - Evaluation.
164.308(b)(1) - Business associate contracts and other arrangements.
164.308(b)(3) - Written contract or other arrangement (Required)

Rule Assessment

Part 164 - Security and Privacy
164 - Subpart C - Security Standards for the Protection of Electronic Protected Health Information
164.310 - Physical safeguards.
164.310(a)(1) - Facility access controls.
164.310(a)(2)(i) - Contingency operations (Addressable)
164.310(a)(2)(ii) - Facility security plan (Addressable)
164.310(a)(2)(iii) - Access control and validation procedures (Addressable)
164.310(a)(2)(iv) - Maintenance records (Addressable)
164.310(b) - Workstation use.
164.310(c) - Workstation security.
164.310(d)(1) - Device and media controls.
164.310(d)(2)(i) - Disposal (Required)
164.310(d)(2)(ii) - Media re-use (Required)
164.310(d)(2)(iii) - Accountability (Addressable)
164.310(d)(2)(iv) - Data backup and storage (Addressable)

Rule Assessment

Part 164 - Security and Privacy
164 - Subpart C - Security Standards for the Protection of Electronic Protected Health Information
164.312 - Technical safeguards.
164.312(a)(1) - Access control.
164.312(a)(2)(i) - Unique user identification (Required)
164.312(a)(2)(ii) - Emergency access procedure (Required)
164.312(a)(2)(iii) - Automatic logoff (Addressable)
164.312(a)(2)(iv) - Encryption and decryption (Addressable)
164.312(b) - Audit controls.
164.312(c)(1) - Integrity.
164.312(c)(2) - Mechanism to authenticate electronic protected health information (Addressable)
164.312(d) - Person or entity authentication.
164.312(e)(1) - Transmission security.
164.312(e)(2)(i) - Integrity controls (Addressable)
164.312(e)(2)(ii) - Encryption (Addressable)
164.314 - Organizational requirements.
164.314(a)(1) - Business associate contracts or other arrangements.
164.314(a)(2)(i) - Business associate contracts (Required)
164.314(a)(2)(ii) - Other arrangements (Required)
164.314(a)(2)(iii) - Business associate contracts with subcontractors. (Required)
164.314(b)(1) - Requirements for group health plans.
164.314(b)(2)(i)-(iv) - Requirements for group health plans. (Required)
164.316 - Policies and procedures and documentation requirements.
164.316(a) - Policies and Procedures.
164.316(b)(1) - Documentation.
164.316(b)(2)(i) - Time limit (Required)
164.316(b)(2)(ii) - Availability (Required)
164.316(b)(2)(iii) - Updates (Required)

Potential PHI Locations

- With PHI potentially in so many places today, the first step is to inventory all potential locations:
  - Portable devices
  - Multi-user workstations in public settings
  - Single user workstations
  - Servers
  - Medical Devices
  - Remote access
  - Cloud remote hosts
  - Wi-Fi
  - Emails
  - Copiers

Potential PHI Locations

- With PHI potentially in so many places today, the first step is to inventory all potential locations:
  - External hard drives
  - Backup tapes
  - BYOD
  - Hardcopy and electronic disposal
  - Other electronic transmissions

Potential PHI Locations

- With PHI potentially in so many places today, the first step is to inventory all potential locations:
  - Affiliated organizations such as:
    - HIEs
    - ACOs
    - Third party business associates (BAs)
    - Population Health
      - Internet of Things
      - TeleHealth / TeleMedicine
      - Patient Portals
  - More……

Need to Analyze and Document

- For each location examine and document:
  - Current controls
    - Administrative (e.g. workforce training, etc..)
    - Physical (e.g. Facility Security Plans)
    - Technical (e.g. Controls and Testing)
    - Organizational (e.g. Policies and Procedures)
  - Future Plans
  - Gaps
  - Risk likelihood and impact
  - Risk mitigation plan

PHI Vulnerability Assessment

Type	Status / Controls	Comments	Future Plan	Gaps (Y or N)	Gap Description	2017 Risk Level (L - Low, M - Medium, H - High)			Risk Level Score	Risk Comment	Mitigate / Action (Y, N, NA)	Mitigation Recommendation
						Likelihood	Impact	Risk	#DIV/0!			
Email	In addition to Microsoft Exchange email encryption using Transport Layer Security (TLS) which encrypts the tunnel or the route between email servers, CE implemented email encrytion solution using fortimail. in order to help prevent snooping and eavesdropping											
Mobile devices (laptops, tablets, smartphones)	CE is not using blackberries anymore, We are using IPhones and purchased Apple Mobile Device menangement software (MDM). Once a phone is enrolled, IT can remotely push updates and wipe phone out if compromised.											
USB flash drives, CD's and external hard drives.	All USB ports and CD/ROM drives are disabled and all workstations are locked, users can use encrypted flash drives provided by IT only as long as no PHI reside on them.											
Multi user workstations - Generic (e.g. used by nursing, medical record coders, etc.)	A new workstation setup was rolled out to the units where users share PCs. The shared PCs are locked down and unique user ids and passwords are mandatory. Generic IDs have been eliminated. Screen Savers time outs set at xx minutes) are being pushed on all Workstations as another security measure.											
Single user workstations	Users have their own ids and passwords to access single user workstations, CD ROMs and USB ports are locked down on those workstations											
Backup tapes	redundancy backup for few important servers we do use tapes for back up. They are rotated and stored in a different building on campus. The tapes are stored inside a cabinet with a combination lock, in a room with a locking entry door. Only technical and operational staff have access to the back-up tapes. Back-up tapes are rotated on a daily basis and stored for an entire month. 30 tapes are kept in storage. Tapes are written over at the end of their 30 day cycle											
Servers on facility network. Physically hosted	Computer room, 1 at Main room, 1 at the hallway that leads to the Main Computer room. Those Cameras are being monitored 24 x 7 by CE Security department and MIS Helpdesk0 Cameras were installed at critical locations, 2 at main Computer room, 1 at Main room, 1 at the hallway that leads to the Main Computer room. Those Cameras are being monitored 24 x 7 by CE Security department and MIS Helpdesk											

PHI Vulnerability Assessment

Type	Status / Controls	Comments	Future Plan	Gaps (Y or N)	Gap Description	2017 Risk Level (L - Low, M - Medium, H - High)			Risk Level Score	Risk Comment	Mitigate / Action (Y, N, NA)	Mitigation Recommendation
						Likelihood	Impact	Risk	#DIV/0!			
Remotely hosted databases (Servers external to the ORG network)	Current SSAE16 documents for remotely hosted databases has been obtained and reviewed by CE											
Wireless transmission - Internal / WIFI	A policy and procedure for CE Guest Network access has been provided											
Remote access transmission	Citrix Remote access from Outside CE instructions and rules is given to any user granted access. Uploaded in CA											
ePHI sent to third parties	Any data transmission to third parties is handled over VPN connection. Any data sent via email is encrypted.											
Patient portal (If applicable)	Portal has been installed and users can access to log in securely (unique userid and password) and view their personal medical information. Passwords must be changed every 90 days.											
Hardcopy PHI disposal / storage	CE has a contract with an outside vendor for hardcopy disposal for the last 6 years. Locked shredding bins are located throughout the facility and emptied periodically by the vendor											
Clinical Engineering devices	Device Audit Controls, Wireless Security,Websense Endpoint DLP and Data Discovery Agent, Hard Drive Shredding , RTLS Tracking											
Copiers	All copiers are password protected. A password is assigned by department. CE owns the copiers and has a service contract											
Cyber Security	[illegible] at rest and in transit (bank for EMR data at rest), internal network vulnerability management, firewalls, internal intrusion detection system, network security monitoring, security management via patch management, Symantec endpoint security, Qualys, application and network monitoring, and email privacy scanning											
Medical Devices	All medical devices are internal and behind protected firewalls											
BYOD	No outside devices are allowed to access information from the CE server											
Electronic media disposal	There is a formal procedure. All electronic media is demagnetized and cleaned or shredded before disposal											
Fax machines	Fax coversheets are used when information is sent out. Fax machines are in secured offices for inbound fax.											
Microfiche (if used)	Kept in locked cabinet. Properly disposed/destroyed when no longer needed.											
Tele-Health Communications	An outside group has access to perform diagnostic reviews. The vendor must sign a BAA and the system requires a unique user name and password for access											

THE TOP TEN!

- Be a *functional* organization by properly funding your information security program
- *Empower* your Chief Information Security Officer (CISO)
- *Conduct* periodic risk assessments (HIPAA rules, OCR Phase 2 protocols, NIST (including Cybersecurity framework), PCI, vulnerability scanning, external penetration testing, phishing exercises, facility physical security, etc.)
- *Implement and maintain* operational policies, procedures and plans (e.g facility security plans, etc.)
- *Educate* the workforce on a periodic general basis and focused as needed
- *Implement* a process to assess third party business associates for information security risk and contracts
- *Mitigate* known risk in the order of highest to lowest
- *Protect vulnerable* PHI in transit and at rest
- *Be prepared* for an OCR audit, now based on phase 2 protocols
- *Be prepared* to respond to an incident

Cyber Security

A Holistic Approach to Information Security: Risk Management and Beyond

October 2017

CYBERBIT
PROTECTING A NEW DIMENSION

Fact Check…

- ✓ Risk Assessments
- ✓ NIST 800 or CSF
- ✓ PCI DSS
- ✓ ISO 27k
- ✓ Business Associates
- ✓ HIPAA Security Rule

Level Set…

Development and execution of Information Security policy

Compliance training

Development of effective Enterprise Information Architecture

IT infrastructure management

Business and IT alignment

Human resources management

Soft Skill Check…

Why do we do it?

What's our objective?

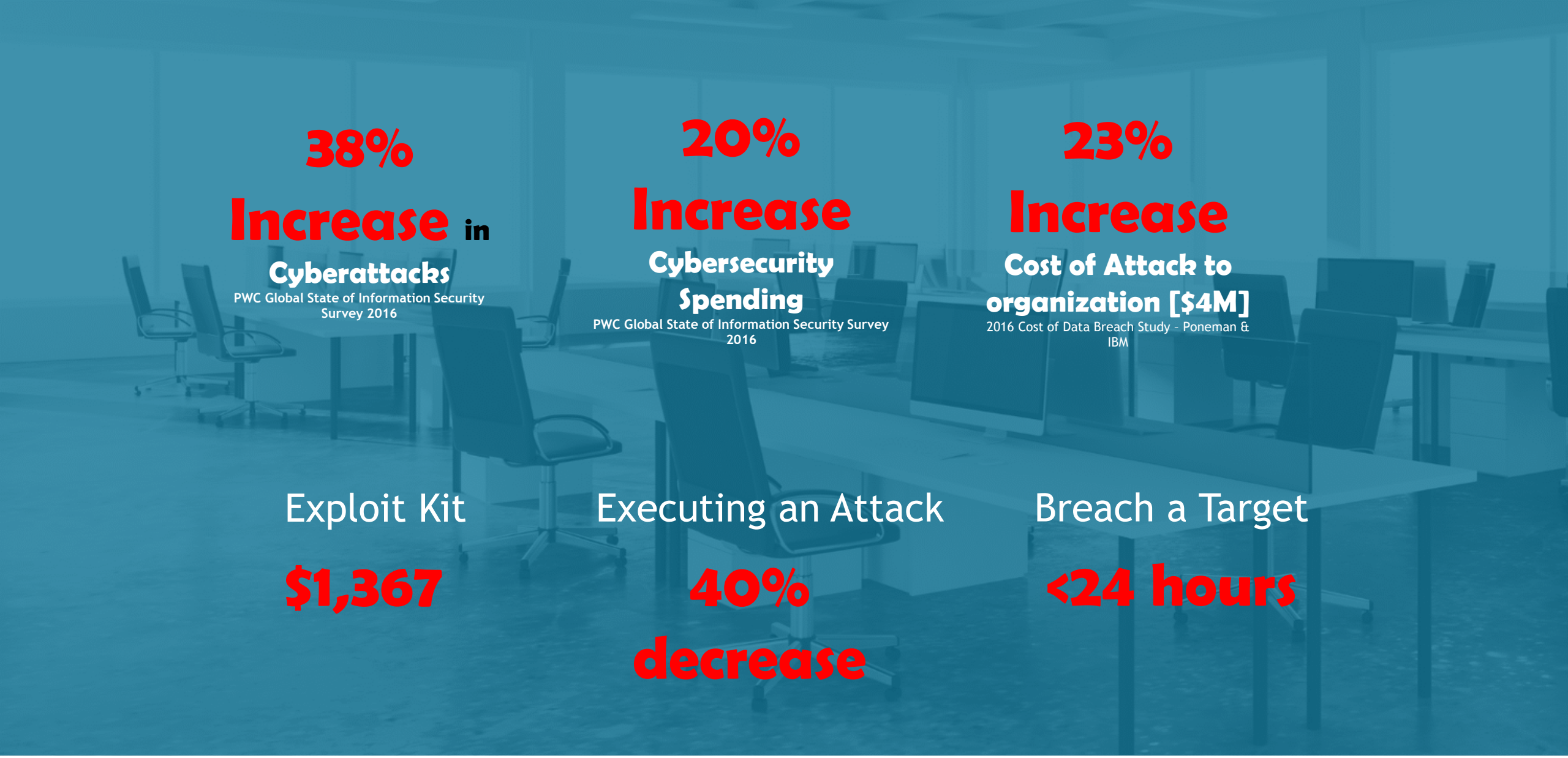
What drives us?

New World Order


Cleveland Medical Associates
Plastic Surgery Associates of South Dakota Ltd
"Make the Beautiful Choice"
mongoDB.
FOR GIANT
Washington State University
Anthem
Nuance
UC Davis Health
Kaleida Health
We see more than patients.
Oral & Facial Surgery Center
Arkansas
Smile like a Champion.
Molina Healthcare
GastroCare
Your gastro health. Our expert care.
ABCD Pediatrics
Torrance Memorial Medical Center
Bronx-Lebanon Hospital Center
Health Care
Medical Oncology Hematology Consultants PA
Diamond Institute
For Infertility & Menopause
Washington University School of Medicine in St. Louis
Lifespan
Delivering health with care.
Harrisburg Gastroenterology, Ltd.
McLaren Health Care
St. Mark's Surgical Center
Indiana Medicaid
PAMC
Pacific Alliance Medical Center
Women's Health Care Group of PA
GLOBAL
The next level of private health insurance

2010 SOLUTIONS FOR 2020 PROBLEMS…


265



38%

Increase in Cyberattacks

PWC Global State of Information Security Survey 2016

20%

Increase Cybersecurity Spending

PWC Global State of Information Security Survey 2016

23%

Increase Cost of Attack to organization [$4M]

2016 Cost of Data Breach Study - Poneman & IBM

Exploit Kit

$1,367

Executing an Attack

40% decrease

Breach a Target

<24 hours

The Changing Landscape…..

What we're seeing….

Fast Moving Attacks

Prolonged Attacks

Keyboard to Keyboard

Fast-moving cyberattacks wreak havoc worldwide

Leaked NSA Tool DoublePulsar Has Infected 200,000+ Computers (April 21 & 24, 2017)

Petya
Malware

Nuance was the victim of NotPetya – a very violent strain of the Petya virus:

Not Petya is not ransomware.

There was no exfiltration of data.

There was no command & control.

The only mission of this attack was to destroy systems using a highly effective cyber munition.

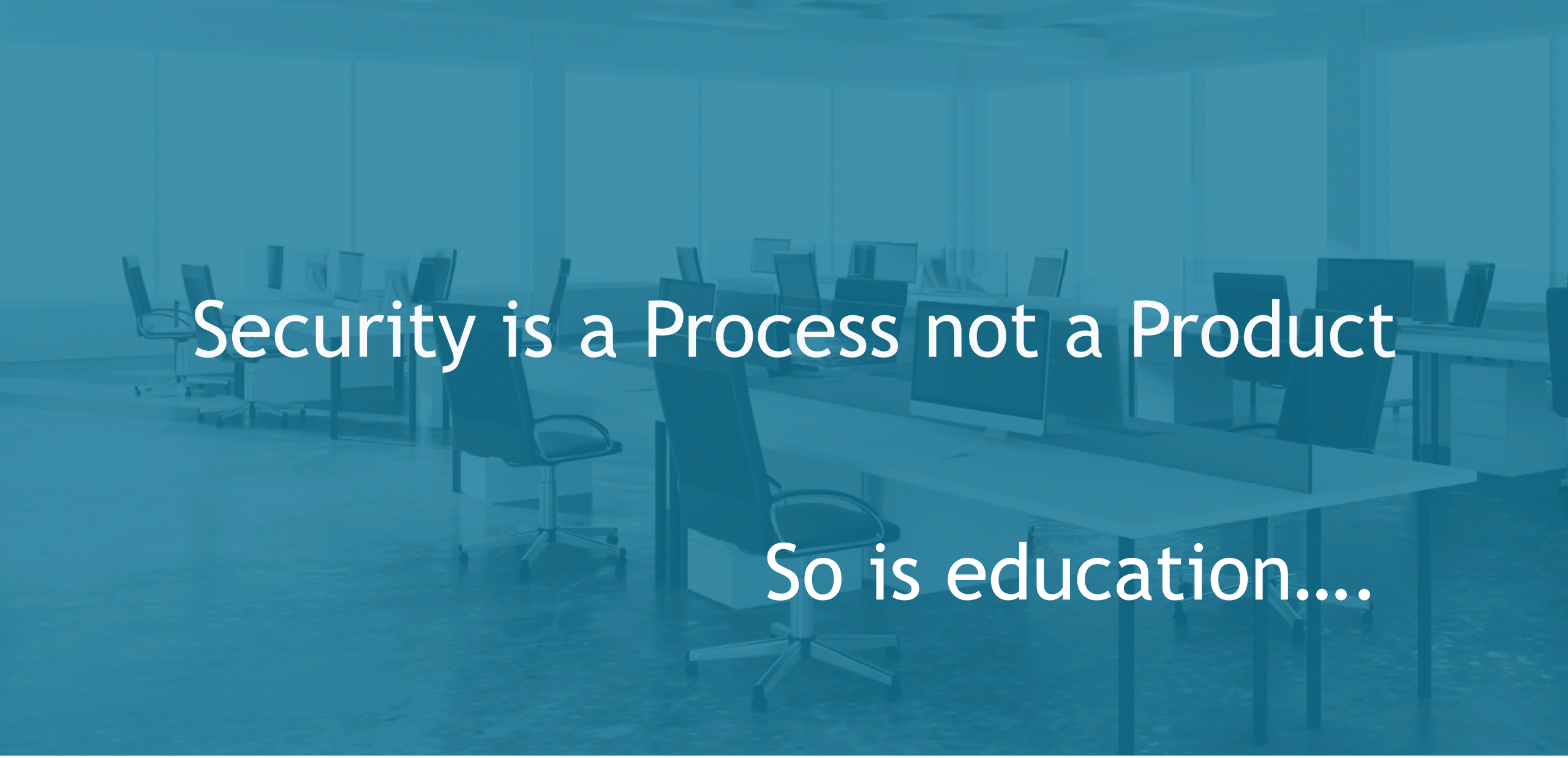
June 27 – 07:00AM EST: A cyberattack is launched

June 27 – 07:14AM EST: The attack is successful and has the following impact:

- 14,800 servers are impacted
  - 7,600 will be destroyed beyond repair.
- 26,000 workstations are impacted.
  - 9,000 will be destroyed beyond repair.

Think Holistic

CYBERBIT
PROTECTING A NEW DIMENSION


Security is a Process not a Product
So is education….

Think Holistic

‘Systems’ are not just the computers

CYBERBIT
PROTECTING A NEW DIMENSION

Think Holistic

Cyber Security Market

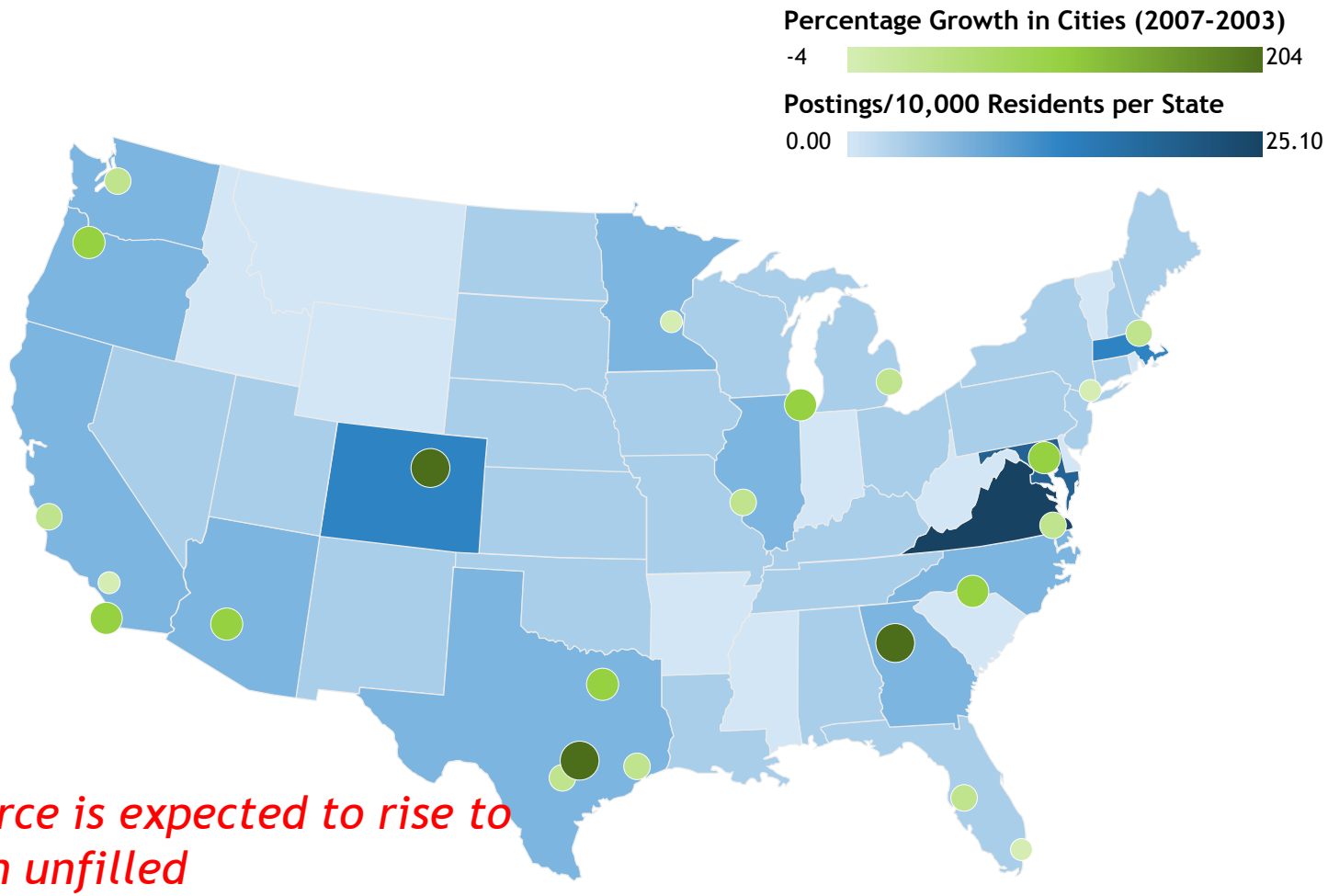
202.36 Billion USD by 2021

CYBERBIT
PROTECTING A NEW DIMENSION

Demand to Fill Cybersecurity Jobs…

More than **209,000 cybersecurity jobs in the U.S. are unfilled**

74% in past 5 years



The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019 with 1.5 million unfilled

(Peninsula Press – Standford, 2015)

This map shows the top 25 cities by percentage growth of cybersecurity job postings. Between 2007 and 2013

Security Leaders' #1 Investment Priority for 2017 is TRAINING

What improvements in IR is your organization planning to make in the next 12 months?

Think Holistic

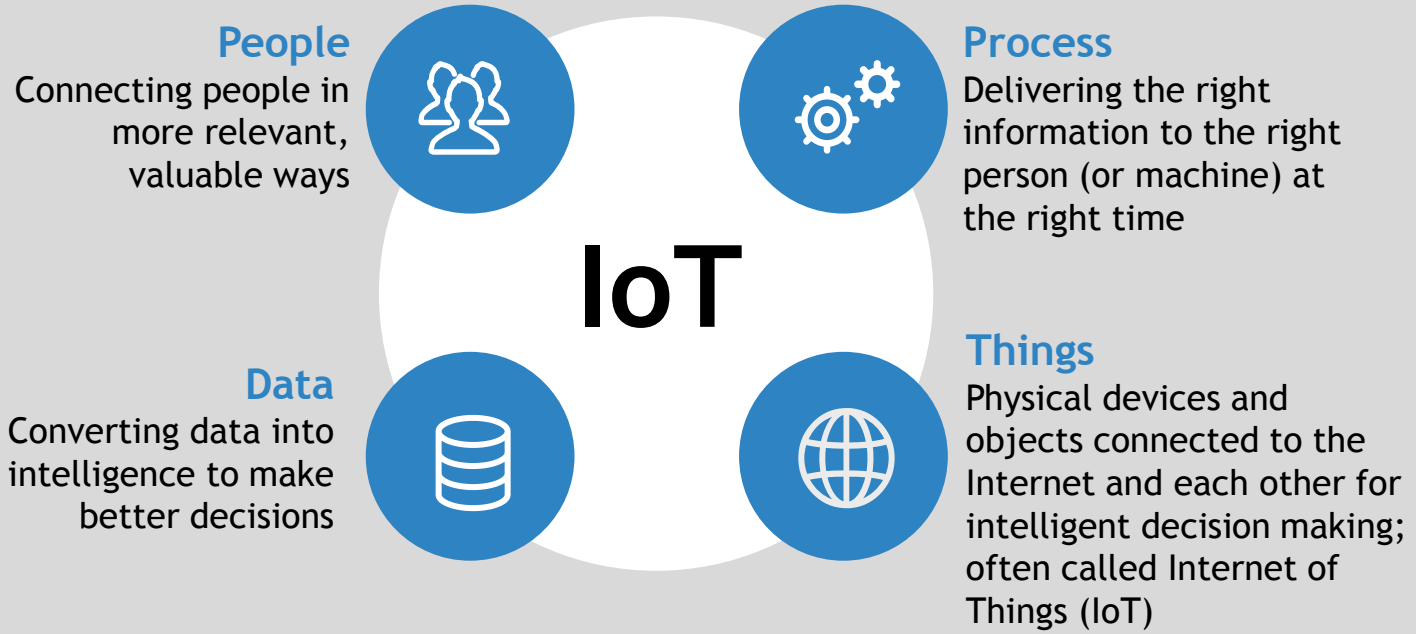
Cybersecurity Skills Shortage is in a State of Emergency

CYBERBIT
PROTECTING A NEW DIMENSION

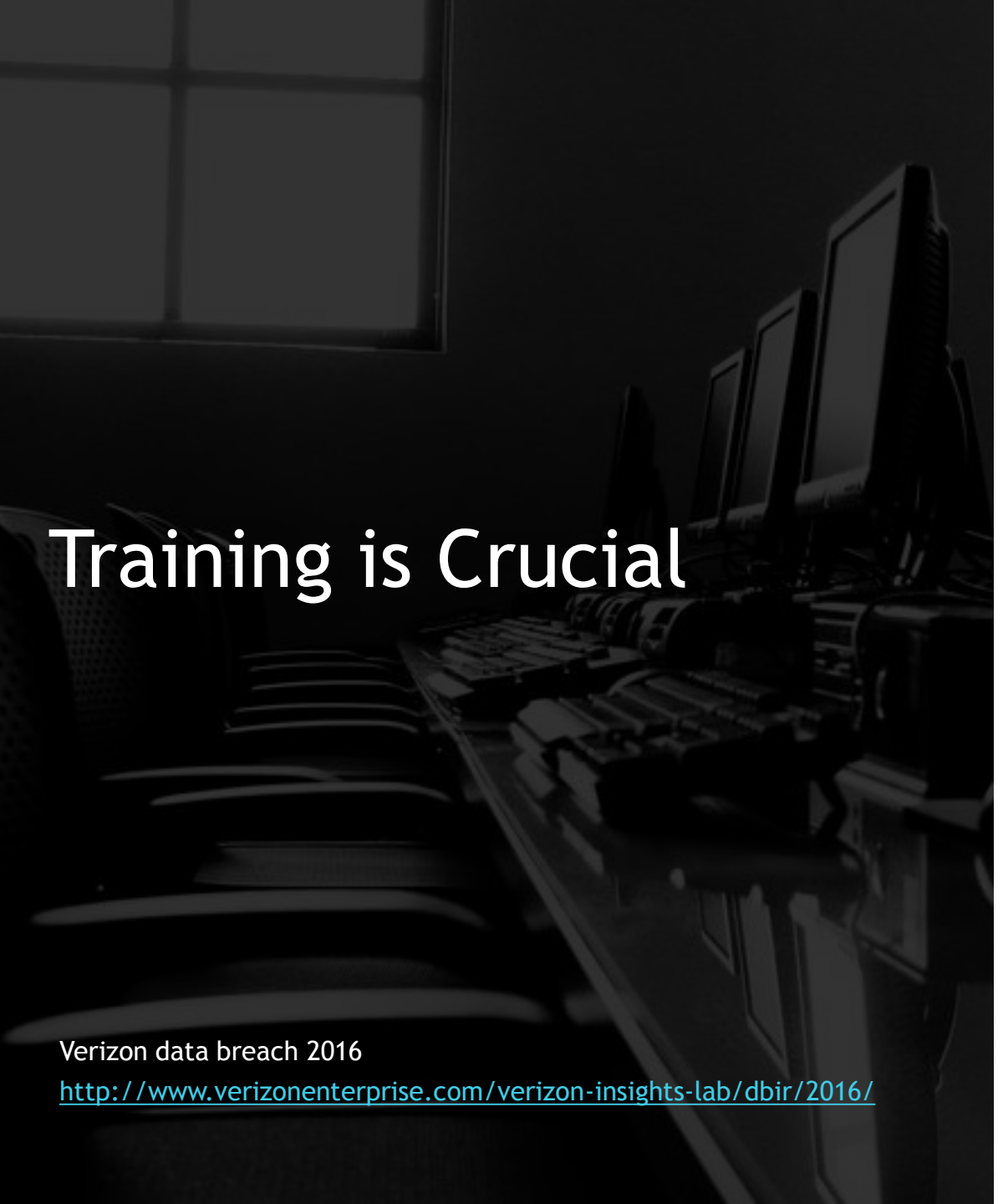
Larger Attack Surface = Larger gap in skills

"As the Internet of Things (IoT) gains more traction, the lack of basic security standards in IoT devices will exacerbate the security skills gap"

Figure 1. With the IoT, Organizations Must Secure a Greater Attack Surface



http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf



Training is Crucial

Verizon data breach 2016
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Threat actors have the upper hand when technology is not maintained and they develop ways to circumvent how it works.

The Need for Prepared Personal

"…the value comes from the people. Software does not provide the answers; it provides the tools."

CYBERBIT
PROTECTING A NEW DIMENSION

What is the biggest barrier to CIOs success?

CIOs see talent (skills and resources) as the No. 1 barrier to their success - 22% of respondents.

Gartner: 2016 CIO Agenda Survey - 7

	Barrier to success as CIO	Percentage of CIOs
1	Skills/resources	22%
2	Funding/budgets	15%
3	Culture/structure of organization	12
4	IT-business alignment	11%
5	Technology challenges (legacy, security, etc)	9%
6	Capacity/willingness to change	8%
7	Management sponsorship/understanding/relationships	8%

Note: Percentages represent the number of CIOs identifying an item as their main barrier.

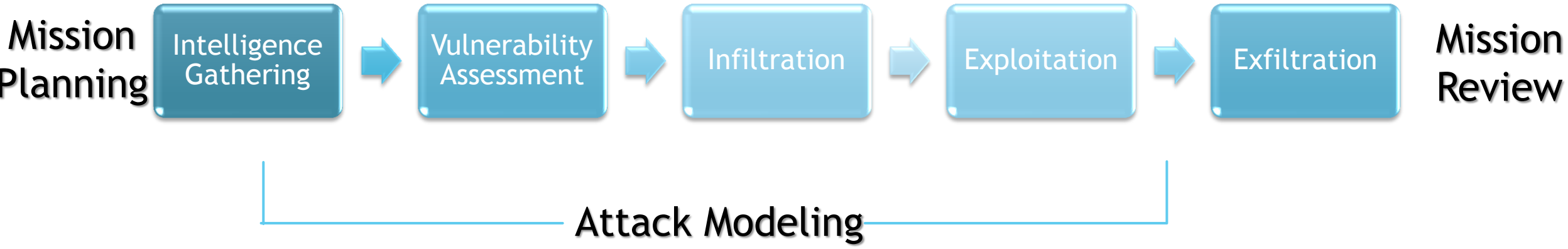
https://www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights_2016.pdf

Closing the Cybersecurity Gap Requires Education

Reform education and training programs to include more hands-on learning

Intel Report
http://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

The Attacker's Perspective



Simulation Models

Tabletop

- Highly Realistic
- Stresses Problem Solving
- Opportunity for Learning and Coaching
- Low Risk to Organizational Operations

Full Incident

- Highly Realistic
- Involves Extended Teams
- Focuses on Operational Response
- Some Risk to Organizational Operations

Cyber Range (Virtual)

- Highly Realistic – C&C / Defend
- Involves Extended Teams
- Focuses on Learning & Operational Response
- Can be customized to emulate production

Incident Response Realities

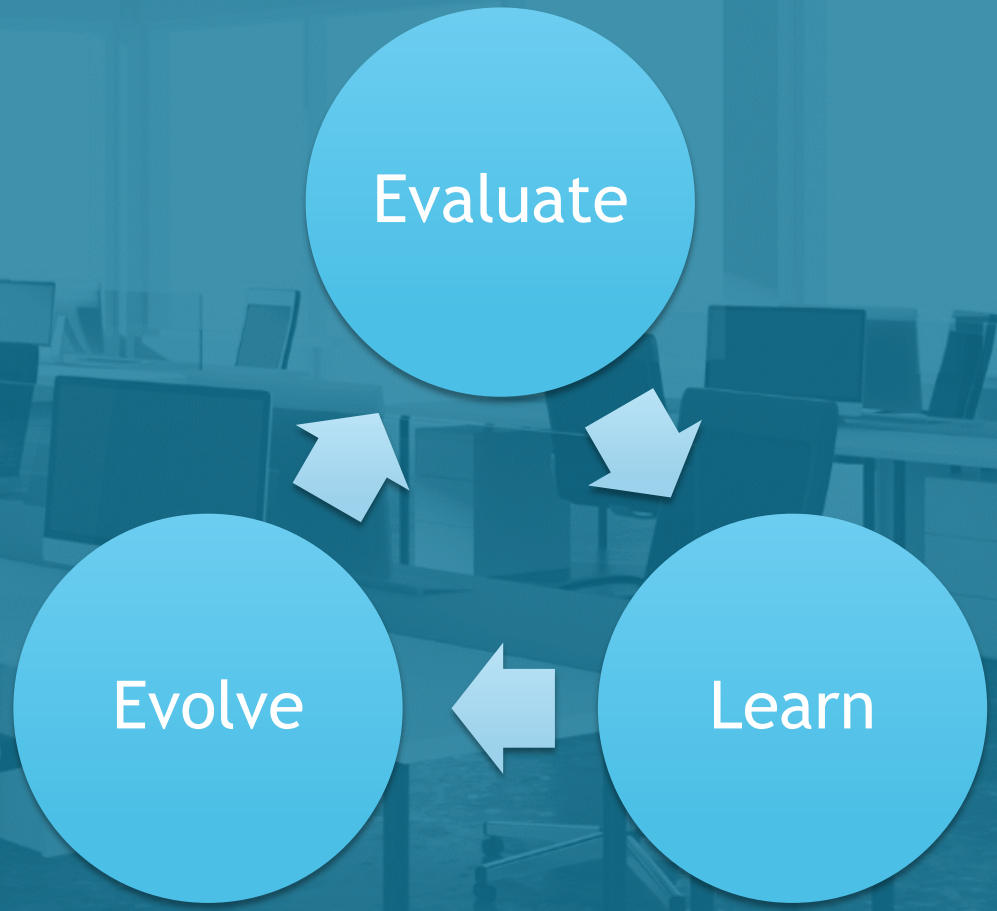
- Most organizations do not have an incident response plan
- Those organizations that do have an incident plan, often times don't:
  - test the plan.
  - base it on current threat intelligence.
  - update it periodically.
  - have adequately trained teams

Cybersecurity Tactical Simulation (Table Top)

Safely analyze ability and readiness in responding to cybersecurity incidents.

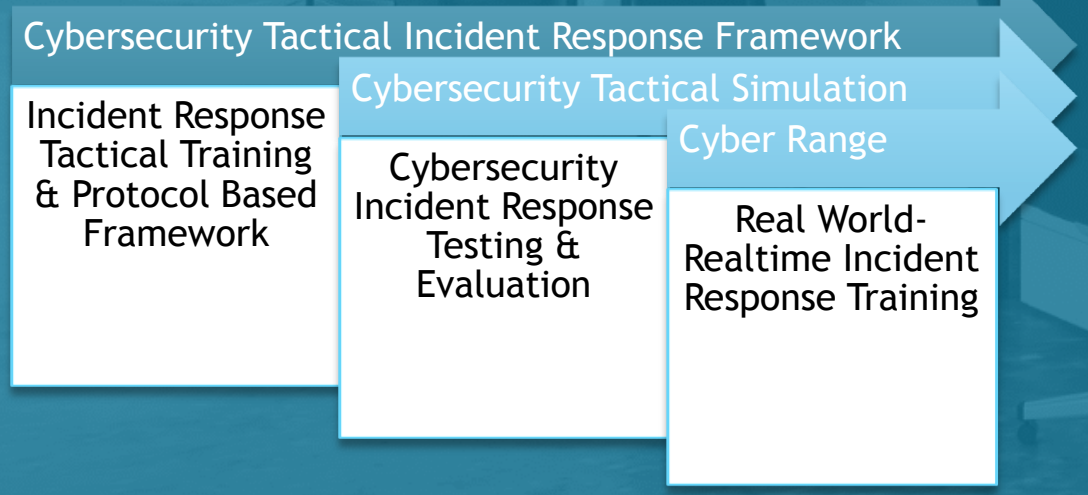
Opportunity to evaluate the maturity of plans, quantify if their teams have the appropriate tools and skills

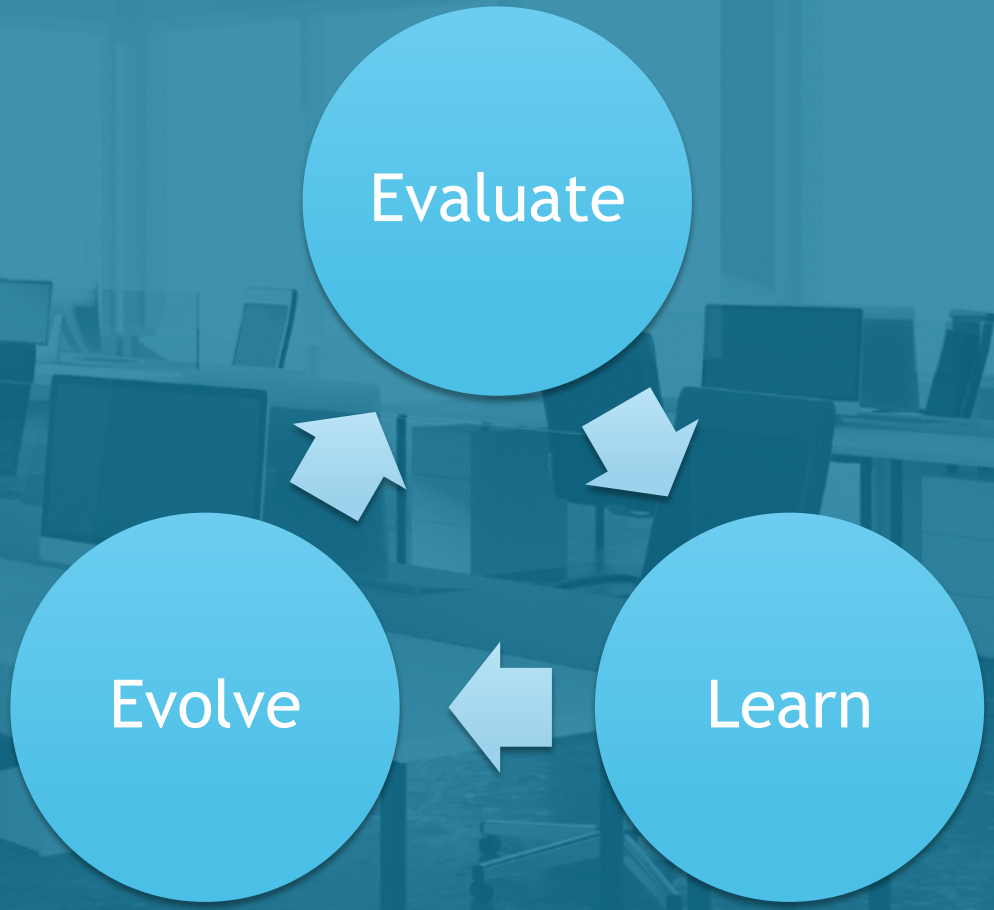
Determine if systems are able to withstand cybersecurity attacks.



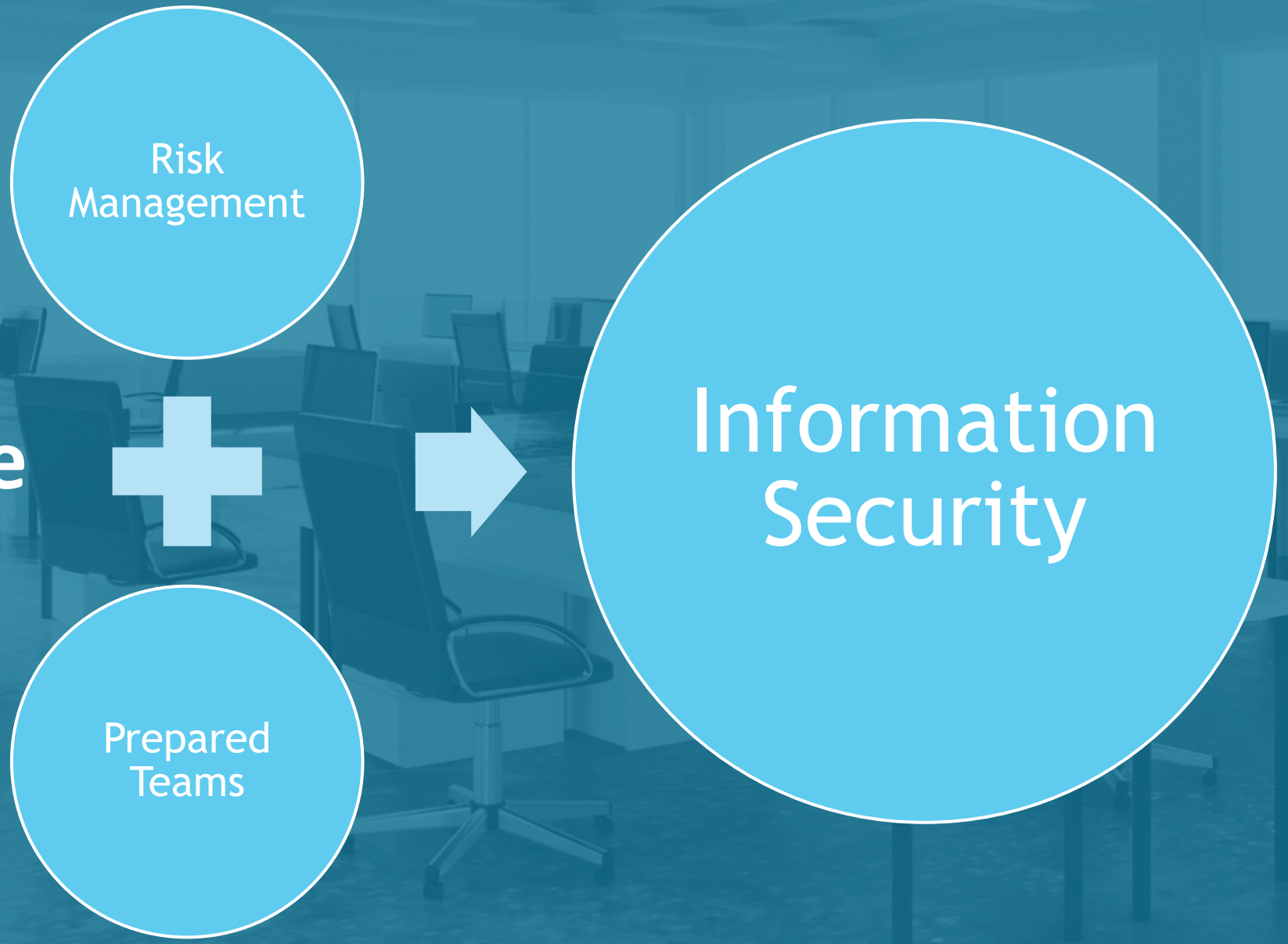
Cyber Range

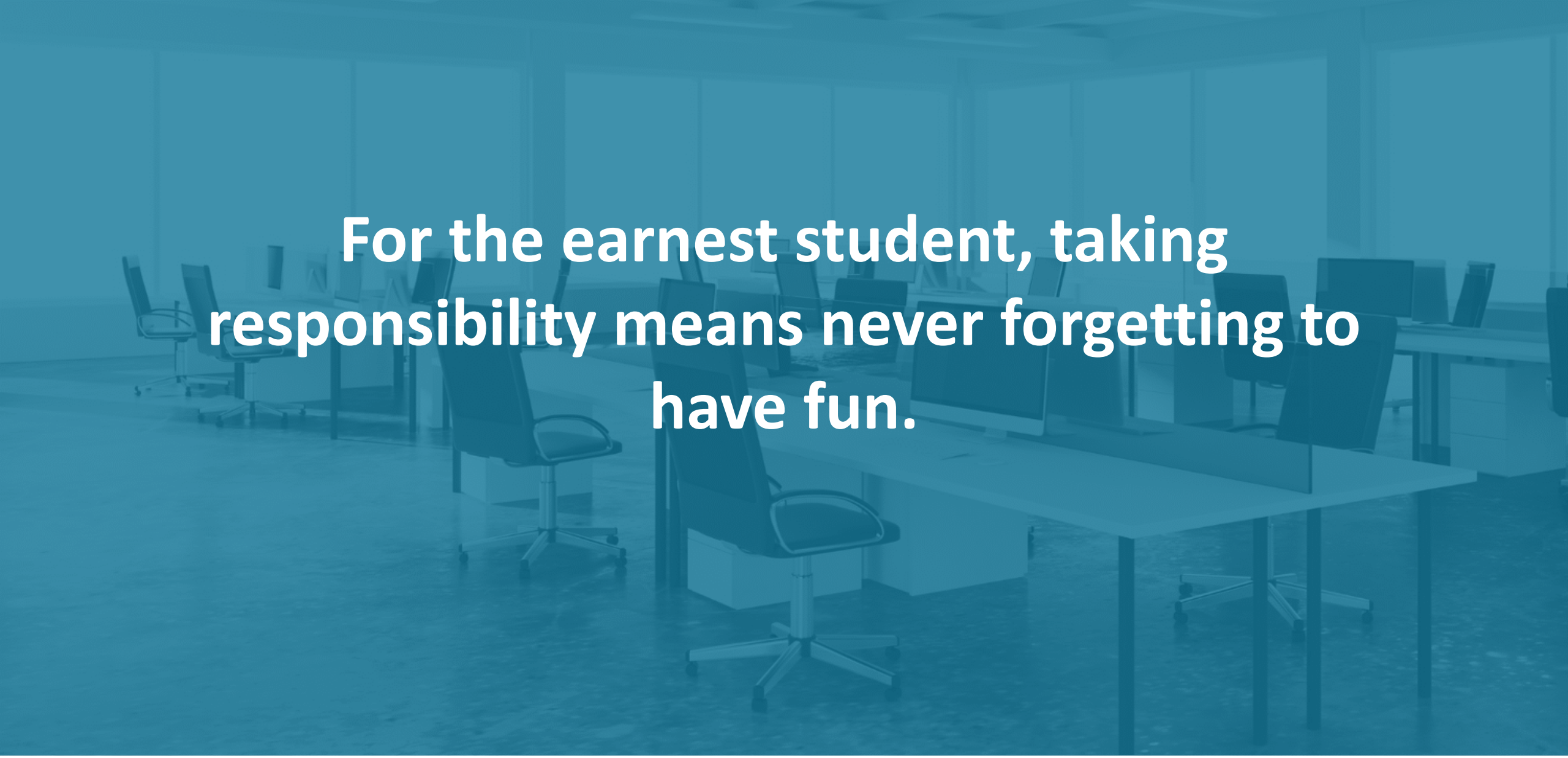
- **Command and Control v. IRT**
- **Virtualized Environment**
- **Rated Responses**





Bring it Home




For the earnest student, taking responsibility means never forgetting to have fun.

Thank You!

For more information on how to use advanced simulation technologies to approach the training market, visit http://go.cyberbit.net/cyberbit-range-learn-how/

CYBERBIT
PROTECTING A NEW DIMENSION

Summing it Up

High Level

Effective Information Security Programs should include:

- An executive mandate
- Organizational governance and accountability
- Assigned responsibility (CISO), independent of IT (reporting to compliance, legal, risk, or internal audit; or where it makes sense for each org)
- Adequate budget – human and controls

High Level

Effective Information Security Programs should include (cont'd):

- Organized evidence of due diligence
- Efficient collaboration for risk assessment and mitigation
- An operational IT contingency plan
- An operational cybersecurity plan
- A comprehensive workforce training program

High Level

What should you spend your money on?

- Risk Assessments
- Technology that detects and stops a breach
- Solutions that keep track of what you are doing to address your critical issues

Motivating Factors

- Reducing the risk of a breach
  - Internal
  - External – (e.g. BA)
- Due Diligence vs. Negligence
- OCR pro-active and reactive audits
- Fear of major $$ penalties and lawsuits
- Protect organizational reputation

Reducing Risk of Breach

- Rule Assessments – standards and implementation specifications
- Risk Assessments and mitigation
  - Technical – e.g. network, encryption
  - Administrative - e.g. ePHI vulnerability assessment, workforce training, BA monitoring, proactive audits
  - Physical – e.g. facilities, workstations

Be Prepared

- Covered entities and BAs should conduct a mock audit in order to be prepared for a real audit
- Need to be able to show documented operational compliance
- Need to drill down on each standard and implementation spec and provide documented proof of operational compliance

Evidence

Be prepared to show evidence:

- Policies and procedures and operational audits
- Workforce training (attendance sheets, eLearning database)
- Risk assessments and mitigation
- Disaster recovery and business continuity plans and tests
- Cybersecurity tactical simulations
- Audits, incidents, and mitigation
- Facility audits and mitigation
- PHI vulnerability assessments and mitigation Information system activity reviews and workforce sanctions for violations, etc..

Future

- Change is the only constant
- More technology
- More vulnerabilities
- More controls required
- More of everything?
- Hopefully less breaches!

Still have questions after the event?

- Feel free to reach out to our presenters with any questions:
- Gerry Blass, ComplyAssistant – (SPC Co-Chair) - gerry@complyassistant.com
- Mike Chirico, Sensato – (SPC Co-Chair) - mike.chirico@sensato.co

Ingredients of a Holistic Approach to Information Security Risk Management

Presented by

Gerry Blass, ComplyAssistant and Mike Chirico, Sensato

HIMSS NEW JERSEY Chapter

TRANSFORMING HEALTHCARE THROUGH IT