CBA
Cybersecurity and Information Assurance Solutions

Managing Risk in a Dynamic Cyber Environment

DAVID SHAW, ASSM, CISRM,
CBA CEO

www.cyberba.net

ENTERPRISE SECURITY
TOP 10 VULNERABILITY MANAGEMENT Solution Providers 2017

CBA INC. – WHAT WE DO

CBA offers professional consulting services covering the entirety of the NIST cyber security framework: Identify, Protect, Detect, Respond, and Recover. We develop a cohesive security posture, which will better protect our clients and enable them to respond more effectively when intrusions into their critical networks occur.

CBA specializes in risk assessment and risk management. Our services are tailored to meet specific needs of our clients.

- ✓ Tabletop Exercise Planning, Administration, and Facilitation
- ✓ Vulnerability, Threat, and Business Impact Assessments
- ✓ Information Security Policy Generation & Modernization
- ✓ Building IT Security Awareness & Training Programs/Content
- ✓ Cybersecurity Focused Business Consulting
- ✓ Regulatory compliance and privacy programs

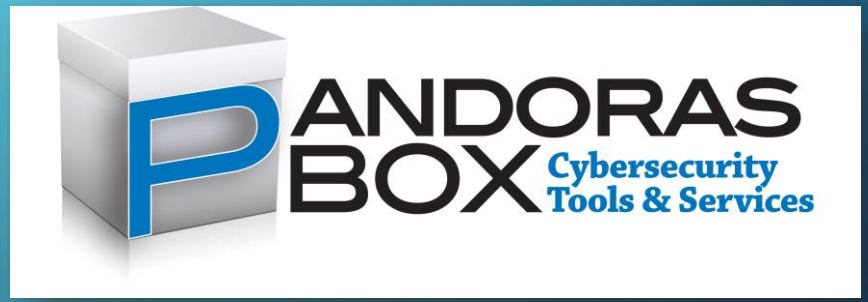
TEG7

CBA
Cybersecurity and Information Assurance Solutions

CBA TECHNOLOGY S0LUTIONS

PandorasBox© (PBX) Cybersecurity Tools and Services is the core technology practice within the CBA family of products and services, it is the center point for all technology products, tools and associated technology services offered by CBA.

- ✓Comprehensive Product Assessments
- ✓Tool and Product Implementation
- ✓Customized Analyst Training Programs
- ✓Network Security Policy Reviews
- ✓Full Spectrum Threat and Vulnerability Assessments



CBA
Cybersecurity and Information Assurance Solutions

Experts worried about ransomware hitting critical infrastructure

'Shock And Awe' Ransomware Attacks Multiply

The unexpected legal consequences of cyber-attacks

'Internet of Evil Things' challenges security pros

Cisco: Data breaches costing some businesses 20 percent of revenue

"Hackers have decided it's easier to end-run an enterprise's multi-million dollar security system and instead simply target an open server."

Survey Says 66% Of Consumers Won't Work With Breached Companies

EU tools up for cyber war

Why 2017 will be the worst year ever for security

60% of breached businesses will fail within 6 months

CBA
Cybersecurity and Information Assurance Solutions

OUR DIGITAL SOCIETY

Each critical infrastructure sector is vast and unique, yet impacts to one will affect all the others. Here are a few examples:

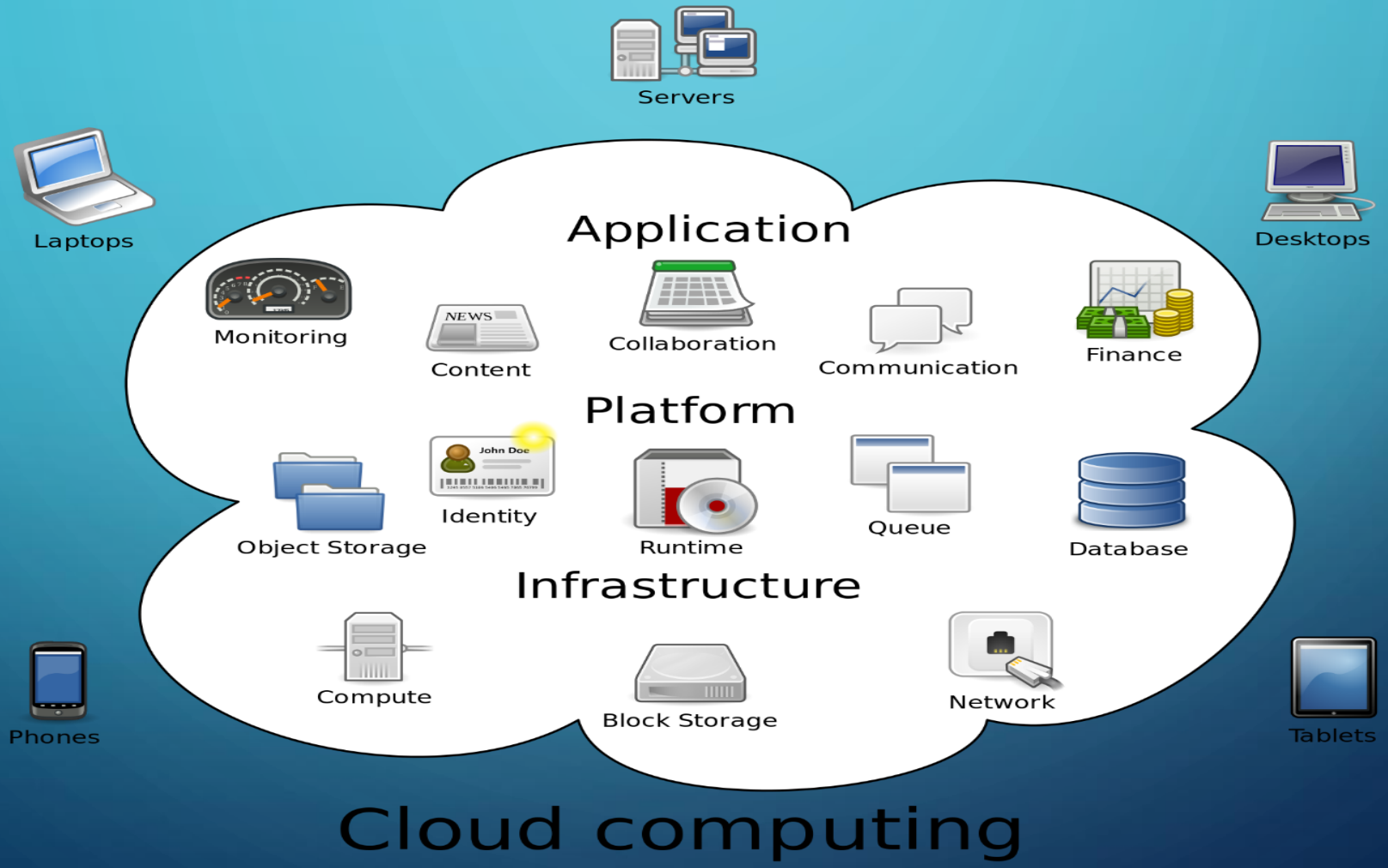
Sector	Interdependency
Critical Manufacturing	**Products made are essential to other critical infrastructure sectors (Includes Transportation Equipment Manufacturing such as Aerospace products and parts)**
Energy	**Provides enabling function across all critical infrastructure sectors. 80 % owned by the private sector.**
Information Technology	**Produce and provide hardware, software, and info. tech. systems and services for all critical infrastructure sectors.**
Transportation Systems	**Including aviation, maritime, and mass transit ensures the movement of people and goods throughout the country and overseas.**

Source: DHS

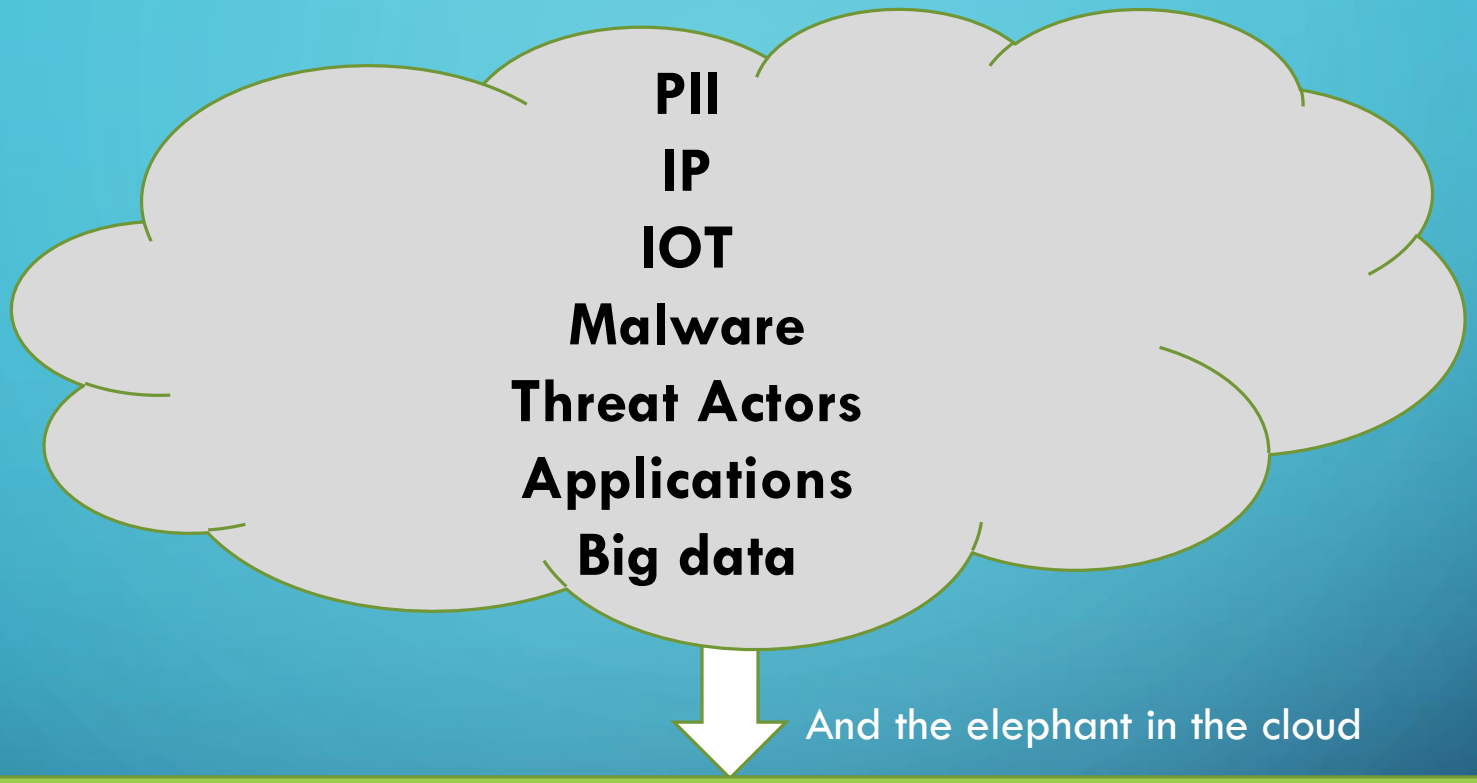
CBA
Cybersecurity and Information Assurance Solutions

HOW WE CONNECT

Cloud Computing enables on-demand access to a shared pool of configurable computing resources which can be rapidly provisioned, accessed and managed with minimum effort.



WHAT IS IN THE CLOUD?



CBA
Cybersecurity and Information Assurance Solutions

INTERNET OF THINGS

- What is the internet of things?
  - Imbedding network technologies into everyday objects so that they can send and receive data
  - TV's, RADIO's, refrigerators, cars, smart meters, toys, doorbells, security systems, air quality sensors, garage door openers, lights, vents, even coffee makers…
- How many devices can be connected to a single router?
  - Theoretically up to 250
  - Reality is limited by bandwidth

Challenges to Securing Data on the Cloud

- Infinite threat surfaces and vectors
- Providers offer varying policy structures and security oversight
- Full enterprise integration can result in breaches causing extreme financial loss, IP exfiltration, and brand damage
- Level of security provided in the cloud environment be equal to or better than the security provided by a traditional IT environment.

CBA
Cybersecurity and Information Assurance Solutions

TECHNOLOGY SECURITY

- Manufacturers in a rush to service the desire of consumers rush product development and delivery

- Security is an afterthought, or generally not addressed directly by the manufacturer

- We then buy tools and "protectors" to provide cybersecurity
  - Average medium sized business has between 50 to 70 tools used to protect the network

CBA
Cybersecurity and Information Assurance Solutions

COMMON CYBERSECURITY DEFINITIONS

- **Threat Actor**
  - Usually a person trying to gain access to your systems, can be another system
- **Threat Vector**
  - The path that the threat actor is going to use to gain access to your system
- **Threat Surface**
  - The sum of all vectors
- **Vulnerabilities**
  - Pinpoints in the surface through which a vector can gain access
- **PII**
  - Personally Identifiable Information (credit cards, SSN, bank account numbers, etc.)

CBA
Cybersecurity and Information Assurance Solutions

COMMON THREAT ACTORS

- APT: Advanced Persistent Threat
  - Usually nation states
    - High capability, ability to stay on networks for years
- Cyber Criminal
  - Out to make money
    - Wide range of capabilities, from very advanced legit, elite hackers to script kiddies
- Hacktivists
  - Out to make a statement
    - Wide range of capabilities, from very advanced legit, elite hackers to script kiddies
- Corporate Spies
  - Hacking for a check
    - Usually going to have a high capability, likely came from an APT

CBA
Cybersecurity and Information Assurance Solutions

COMMON THREAT ACTORS CONT'D

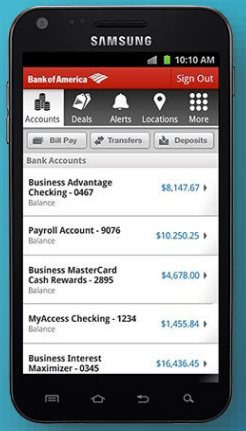
- **Nation States / Governments**
  - Industrial espionage, malicious hacking, theft of PII
- **Vandals**
  - Bragging rights, ego, ego ego
    - Usually low technical capability, defacing websites and such
- **Insider threats account for 60% - 80% of incursions**
  - Can range from malicious intent to "accidents"
    - Inside your home this can be significant others behaving badly on computers
    - In Business…this can be devastating

COMMON THREAT VECTORS

- **Phishing**
  - Trying to get you to click on emails, then directing you to a website for exploitation
- **DDOS**
  - Using networked systems to deny service
- **Malware/ransomware**
  - Once the software is installed it locks up your machine
- **WIFI**
  - The world is networked on WIFI
  - Security is there, but depends on the user, and can usually be breached with little effort
- **Thumb drives**
  - Often infected with embedded virus - connects and exchanges data in milli-seconds
- **Brute forcing passwords**
  - Pretty easy if your password is password (or any derivation of that)

CBA
Cybersecurity and Information Assurance Solutions

MOBILE DEVICES



- Characteristics of a Mobile Device
  - Handheld or portable (Ex. phones, laptops, Tablets)
  - Capable of Data transmission
- Vulnerabilities of Mobile Devices
  - Connects to the internet
  - Executes code
  - Connects to unsecured IOT (Ex. your car)

- Securing your mobile devices
  - Update your software, use strong passwords or biometrics, avoid open Wi-Fi hotspots, enable remote wipe, avoid 3rd party apps

CBA
Cybersecurity and Information Assurance Solutions

PERSONAL RESPONSIBILITY

- At work: BYOD (Bring your own device)
  - What's on your device?
    - IP, Confidentiality, PII/customer data
  - Policies and Procedures for your company as it pertains to security?
- At home
  - Securing WIFI
  - IOT devices can be used as part of a DDOS
  - Legal requirements for devices in your home?
    - None, but it is best practice to secure your devices

CBA
Cybersecurity and Information Assurance Solutions

SECURITY IN THE WORKPLACE

- Educate yourself, and your coworkers
- Use firewalls, antivirus, and email protection
- Don’t plug just anything into your computer, scan it first
- Passwords
  - Use them and love them
  - Make them long, and complex
  - Write them down, and store them in a safe place
  - Avoid reuse of the same password for multiple devices

CBA
Cybersecurity and Information Assurance Solutions

RISK MANAGEMENT RESOURCES

The Global Risks Report 2017 12th Edition

WORLD ECONOMIC FORUM

Guide for Applying the Risk Management Framework to Federal Information Systems
A Security Life Cycle Approach

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

NIST 800-37

Framework for Improving Critical Infrastructure Cybersecurity

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Supply Chain Risk Management Practices for Federal Information Systems and Organizations
NIST Special Publication 800-161

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

CBA
Cybersecurity and Information Assurance Solutions

NIST 800-53 REVISION 4:
RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

- Trusted by Leading Government Agencies - HHS, CMS, DOD, DHS, State and Local Governments
- IT Compliance and Regulatory Compliance is one of the greatest challenges faced by organizations today.
- Compliance standards such as NIST 800-53, PCI DSS , FISMA, GLBA, SOX, STIG and HIPAA require organizations to secure their networks, harden servers and desktop computers thus ensuring a high levels of security for their confidential enterprise assets and provide network compliance audit reports to auditors when demanded.
- It is critical for organizations to observe the regulatory compliance audit guidelines since being non-compliant to the security and regulatory standards can result in severe penalties or loss of an ATO (Authority to Operate).
- To meet all security and compliance requirements, organizations are required to take proactive measures to establish network security processes for detecting network anomalies, attacks and other vulnerabilities that can cause harm to the sensitive information of the enterprise.

CBA Cybersecurity and Information Assurance Solutions

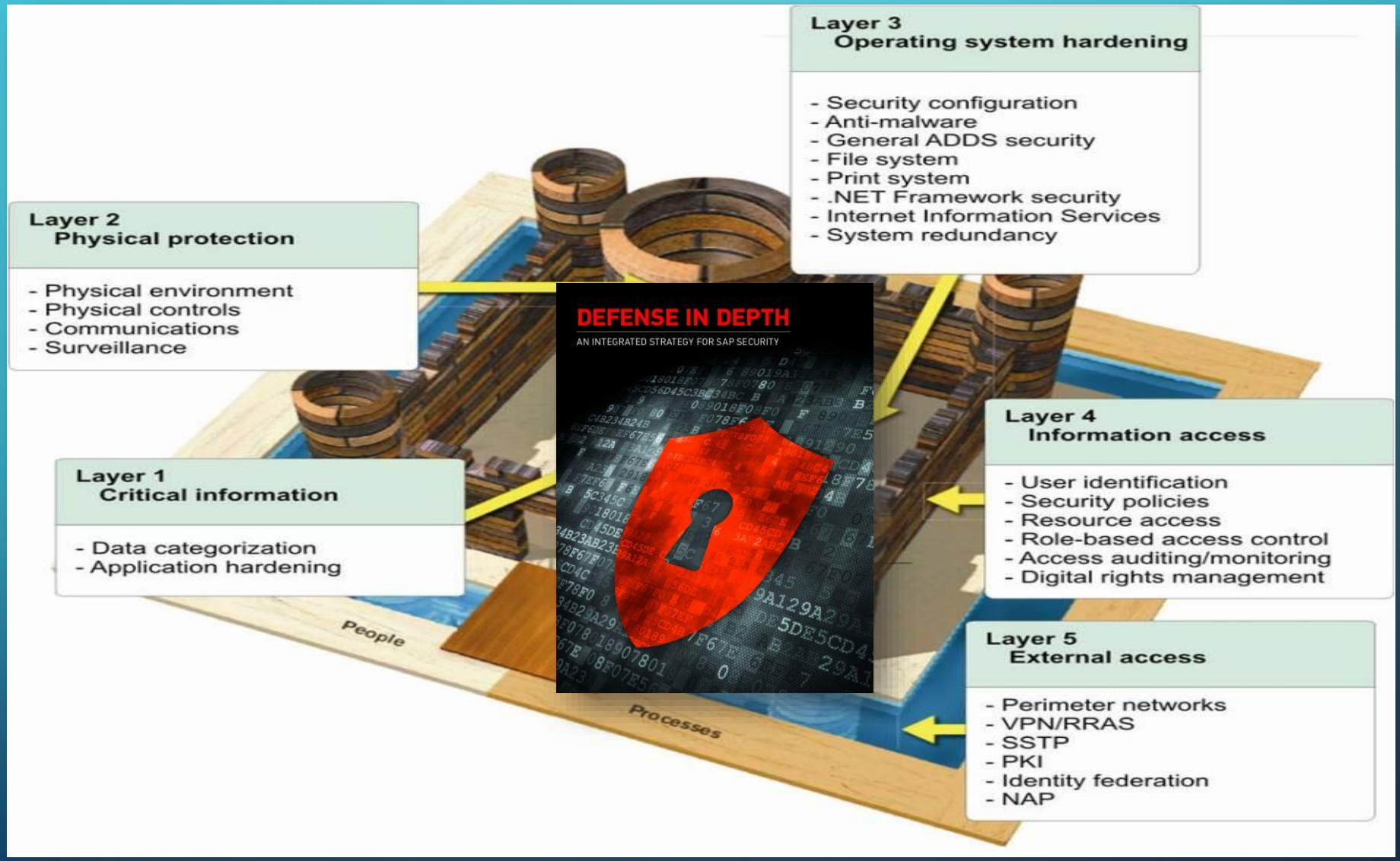
COMPLIANCE STANDARDS SUCH AS NIST 800-53, PCI DSS , FISMA, GLBA, SOX, STIG AND HIPAA

- Audits and Gap Analysis can be performed on-site, remotely, or a combination of both. The typical process will take three to five days to complete depending on the audit level required. The process will include:
  - Meet with the stakeholders to determine what level of auditing is required and set the expectations.
  - Review policies and procedures
  - Perform security and compliance audits
  - Analyze the audit results and prepare the necessary reports and recommendations
  - Meet with the stakeholders and review the audit results and recommendations
  - Prepare a after-action report identifying all issue with recommendations to mitigate any negative findings
  - Work with the client to prepare and implement a mitigation strategy
  - Reexamine the areas that required mitigation to ensure compliance
  - Prepare final report

CYBER THREAT RISK CONSIDERATIONS

The cyber adversary is often well organized, motivated, funded, and persistent in pursuing their goals

A Typical Information Security Defense Model



Source: Reust

No matter how solid the walls of defense…

are

It WILL happen…Probability of One

What matters is how prepared you are to mitigate what occurs

CBA
Cybersecurity and Information Assurance Solutions

CRITICAL INFRASTRUCTURES AT RISK

DDOS ATTACK

CBA
Cybersecurity and Information Assurance Solutions

OUR CORE REQUIREMENTS FOR CYBERSECURITY

- ✓ Enterprise wide understanding of the threats (C-suite)
- ✓ Consistent & periodic reviews of enterprise & system risk postures
- ✓ Updated policies & procedures
- ✓ Integration of cutting edge tools & tradecraft
- ✓ Engagement with industry ISACs
- ✓ Partnerships with US Secret Service ECTF & other law enforcement agencies
- ✓ Retention of highly trained security practitioners
- ✓ Continuous training & testing exercises

CBA
Cybersecurity and Information Assurance Solutions

ACHIEVING PREPAREDNESS & RESILIENCY

Risk Management and Cybersecurity is a Culture…it is a journey, not a destination

CBA Cybersecurity and Information Assurance Solutions

MOVING FORWARD…

~~BUILD FIRST, SECURE LATER…~~

As industry races towards innovation, cyber security professionals lag further and further behind.

We need to develop a robust understanding of defense resilience and encourage a keen awareness on how to combat the asymmetric cyber threat

CBA
Cybersecurity and Information Assurance Solutions

THE BOTTOM LINE IS…

WE ARE ALL AT CYBER RISK… THEREFORE WE ARE INVOKING A PROCESS THAT IS DYNAMICALLY COOPERATIVE IN CREATING A RESILIENT DEFENSE, AND IN SO DOING SEIZES THE INITIATIVE IN CREATING INNOVATIVE PROTECTIONS FOR ALL CRITICAL INFRASTRUCTURES.

CBA
Cybersecurity and Information Assurance Solutions

- David Shaw

  dshaw@cyberba.net

- John Roach

  jroach@cyberba.net