The 4th Annual Information Assurance Day
November 10, 2011
Delaware Room – HUB – IUP

Time Slot	Speaker	Topic Title
8:40 – 9:00	Dr. Deanne Snavely, Dean College of Natural Science and Mathematics	*Opening Remarks*
9:00– 9:45	Mr. David C. Brown - Business CyberSecurity, Inc.	*Four Essential Requirements for Securing Your Enterprise*
9:45 – 10:45	Mr. Greg Porter - Allegheny Digital and Mr. Matthew Stewart - Robert Morris University	*Making sense of the security data generated by multiple devices* *Using open community software to identify network based security risks to sensitive Information*
10:45- 11:00	Break	
11:00-12:00	Mr. Mark Yanalitis – Highmark, Pittsburgh	*Red Teaming approaches, rationales, engagement risks, and methodologies*
12:00-1:00	Lunch Break	
1:00-2:00	Special Agent Jason Pearson and Special Agent Keith Mularski - Pittsburgh Division of the Federal Bureau of Investigation (FBI)	*What keeps me up at night?*
2:00-3:00	Mr. Harley Parkes - NSA	*TBA*
3:00-4:00	Mr. Douglas Brown - First Commonwealth Bank, Indiana	*Information Assurance, an IT Audit Perspective*

For more information, please contact Dr. Rose Shumba, Director, Institute of IA Education, shumba@iup.edu,724.357.3166

BIOGRAPHICAL INFORMATION

DAVID C. BROWN

David C. Brown, CISSP, PMP, CEH, is the president and founder of Business CyberSecurity, Inc., www.BusiessCyberSecurity.com. He is also the inventor of its innovative business information framework model and analysis methodologies. He has more than thirty years of experience in information technology and analysis of business processes combined with more than twenty years of addressing information security issues. He has held a wide variety of engineering, consulting, and management positions in small and large companies.

He holds a Six Sigma Green Belt and ITIL Foundations certification, has earned a Bachelor of Science in management information systems, a certificate in Computer Forensic Technology, and an Associate's Degree in Electronics and Computer Technology.

GREG PORTER

Greg Porter is the founder of Allegheny Digital, a Western Pennsylvania based information security company specializing in network infrastructure security, incident response, enterprise risk management and managed security services. For the past several years, Mr. Porter has both led and delivered comprehensive assessment activities that monitor, test and audit the effectiveness of information system security, risk managed governance and controls, and regulatory conformance. He holds a Bachelor of Science degree in Chemistry from the University of Pittsburgh, a Master of Science degree in Information Technology (Information Security Concentration) from Carnegie Mellon University and a Master of Science degree in Health Care Policy and Management (Highest Distinction) also from CMU. In addition, Mr. Porter maintains several information security related certifications and is a Certified Information Systems Security Professional (CISSP) and a Certified Information Security Manager (CISM).

MATTHEW STEWART

Matthew Stewart is the Director of Information Security at Robert Morris University. In addition, he is an adjunct professor teaching Computer Security, Intrusion Detection, and Computer Forensics.

Matthew earned his Master's Degree in Information Security and Assurance and also holds undergraduate degrees in Information Systems Security and Computer Forensics. He holds several leading industry certifications including the Certified Information Systems Security Professional (CISSP), SANS GIAC Certified Intrusion Analyst (GCIA), and the SANS GIAC Certified Incident Handler (GCIH). He is a member of SANS Advisory Board and is a local SANS Mentor in Pittsburgh.

MARK YANALITIS

Mr. Yanalitis has held positions in the private and public sector as a network security engineer, a Big-4 accounting firm security consultant, and Director of Security for a large regional ISP/MSP. He currently functions as an Enterprise Technical Consultant fulfilling the role of IT Infrastructure Architect for a national health insurance concern. His efforts have concentrated upon enterprise security architectures, threat management, Intelligence life cycle management, and incident response.

Mr. Yanalitis has presented material at INFOWARCON, ISSA, CMU/SEI SOA workshop, DOJ/FBI Quantico, and ISACA. Past committee membership include National Cyber-Forensics Training Alliance - a joint public-private forensic computing cooperative based in Pittsburgh; the NIST/URAC Healthcare Security Workgroup, and former “At-Large” member of the Board of Directors Pittsburgh Infragard. Presently, he is a committee member on the FS-ISAC Portal Product Selection workgroup and public relations point of contact for the newly formed Pittsburgh Chapter of Open Web Application Security Project (OWASP). He is the founder of the LinkedIn Open Source Intelligence Professionals Group – an international professional group dedicated to open source intelligence methods and tradecraft.

Mr. Yanalitis is a member in good standing with the Association for Computing Machinery (ACM), Armed Forces Communications Electronics Association (AFCEA), and Federation of American Scientists (FAS). He holds CISSP designation and IAM recognition by the Information Security Assurance Training and Rating Program (ISATRP). He has held various vendor technical certifications. Mr. Yanalitis is a graduate of the 8th Pittsburgh FBI Civilian Academy program, and the Duquesne University Wecht Forensics Science and Law program. He holds graduate degrees from the University of Pittsburgh and American Military University.

SPECIAL AGENT JASON PEARSON

Jason Pearson is a Special Agent assigned to the Pittsburgh Division of the Federal Bureau of Investigation (FBI). Prior to joining the FBI, Mr. Pearson formed an Information Technology firm out of Chicago, Illinois. As proprietor of the company, Mr. Pearson led a variety of IT security investigations, and worked as a network/systems engineer. In 2009, Mr. Pearson joined the FBI and was assigned to the Bureau's Cyber Squad and High Tech Crimes Task Force where he currently investigates both National Security and Criminal Cyber Crime offenses.

Mr. Pearson is currently on the front line of investigations involving some of the largest and most complex financial fraud schemes to date and has assisted on a number of investigations involving Counter Intelligence and Domestic Terrorism matters. Mr. Pearson's expertise involves sophisticated Botnets and Malware, Computer Intrusion matters, and Automated Clearing House (SACH) fraud.

SPECIAL AGENT KEITH MULARSKI

Keith Mularski is a Supervisory Special Agent assigned to the Pittsburgh Division of the Federal Bureau of Investigation (FBI). Mr. Mularski received his appointment to the position of Special Agent with the FBI in 1998. After attending the FBI Academy in Quantico, Virginia, Mr. Mularski was assigned to the FBI's Washington Field Office where he investigated National Security Matters for seven years. During this time Mr. Mularski worked on a number of high profile investigations such as the Robert Hanssen espionage investigation and the 9/11 Terrorist attack on the Pentagon.

In 2005, Mr. Mularski transferred to the FBI's Cyber Division and was detailed to the National Cyber-Forensics and Training Alliance (NCFTA) in Pittsburgh, Pennsylvania. While detailed to the NCFTA, Mr. Mularski successfully worked with Private Industry Subject Matter Experts on a number of joint Cyber-Crime initiatives with an emphasis in the development of proactive targeting of organized international Cyber-Crime groups. From 2006 through 2008, Mr. Mularski worked undercover penetrating cyber underground groups which resulted in the dismantlement of the Darkmarket criminal carding forum in October 2008. In 2010 Mr. Mularski received the FBI Director's Award for Excellence in Outstanding Cyber Investigation.

In 2011, Mr. Mularski transferred to the FBI's Pittsburgh Field Office. Mr. Mularski is currently the supervisor of the Cyber Squad which responsible for all Cyber investigations in Western Pennsylvania and West Virginia.

HARLEY E. PARKES

Chief, Mission & Technical Vulnerability Office
National Security Agency/Central Security Service

CURRENT POSITION: Mr. Parkes, a member of the Defense Intelligence Senior Executive Service, is the Chief of the Mission and Technical Vulnerability (MTV) office in the Information Assurance Directorate (IAD) of the National Security Agency. The MTV organization conducts Communications Security (COMSEC) monitoring and Technical Security Evaluations to evaluate the overall security of U.S. Government communications and operations. As MTV Chief, he also serves as the Director of the Joint COMSEC Monitoring Activity (JCMA) which operates an enterprise of monitoring centers located throughout the world.

EDUCATION: Mr. Parkes holds a Bachelor of Science degree in Computer Science from the University of Maryland.

PRIOR POSITIONS: Mr. Parkes has worked in the cryptologic career field for 30 years. He started his career in the U.S. Air Force as a collection officer. In January 1983 he was hired by NSA and served in a number of technical and supervisory positions within the Directorate of Operations between 1983 and 1995. In June 1995, he was assigned to NSA/CSS Pacific and spent four years providing cryptologic support to USCINCPAC and PACOM's service components. In 1997 he established, and became the first ever lead of, the Computer Network Vulnerability Team at NCPAC. This team provides computer network security consultations in support of USCINCPAC and its components. In 1999 he returned to NSA Headquarters to continue this work within the Vulnerability Analysis and Operations group of IAD. He became D/Chief of the Operational Network Vulnerabilities (ONV) office in October 2008. The ONV works to strengthen DoD and the national security communities' operational networks through vulnerability assessments, in-depth technical analysis, and long-term integrated best-practice community security solutions. In 2010, Mr. Parkes became Chief of the MTV.

PROFESSIONAL BACKGROUND: He serves as the NSA representative to the Enterprise Solutions Steering Group (ESSG) and is a member of the Technical Advisory Board for the Tower Federal Credit Union

PERSONAL: Mr. Parkes was born in Washington, PA. He resides in Harford County, Maryland with his wife Michelle and their two children, Tyler and Kaylee. He enjoys softball, football and coaching his son's little league baseball team.

DOUGLAS BROWN

Doug graduated from IUP in 1981 with a major in MIS and minors in Economics and Accounting. Since that time he has worked for several financial institutions in several states all in the field of Information Technology Auditing. He started his career as an audit programmer analyst where he worked closely with operational and external auditors learning the audit profession. He created unique audit tests to verify data integrity. He ascertained from his tests that company information had a personality quality to it that permitted a unique view of a company especially in regards to how effective and efficient a company operated. He also was able to expose frauds, errors, misuse of system features, and reveal improperly designed application systems. Doug has also conducted numerous audits of technology systems, applications, production processes, regulatory and compliance directives, product and system life cycles, and service providers. Doug has assisted IT, Executive Management, and the Board of Directors in developing Risk Management and Governance practices. Doug currently is the Senior Vice President and IT Audit Senior Manager for First Commonwealth Financial Corporation located here in Indiana, Pennsylvania.

ABSTRACTS

DAVID C. BROWN
Topic: Four Essential Requirements for Securing Your Enterprise
Abstract:
What makes cybersecurity so difficult for the defenders? If the government, with all of its resources repeatedly gets hacked, what can you do to defend your enterprise? We will show you a new approach to cybersecurity that will change your perspective and help your organization to build better defenses.

MATTHEW STEWART (Matt) and GREG PORTER (Greg)
Topic: Making sense of the security data generated by multiple devices
Abstract (Matt)
In this talk we will discuss how to make sense of all of the security data generated by multiple devices. We can gain a clear picture of meaningful attacks and how to mitigate them through the aggregation and correlation of data collected from key points on the network including firewalls, intrusion detection systems, hosts and vulnerability assessment solutions.

Abstract (Greg)
Topic: Using open community software to identify network based security risks to sensitive Information
Abstract:
The theft of sensitive information continues to challenge both the public and private sector alike. Adequate network situational awareness can provide the difference between detecting a hacking/IT incident or potentially ending up as a statistic on the Dataloss db website. This presentation will provide key considerations for using open community software to identify network based security risks to sensitive information.

MARK YANALITIS
Topic: Red Teaming approaches, rationales, engagement risks, and methodologies
Abstract
The presentation discusses Red Teaming approaches, rationales, engagement risks, and methodologies. “Low-and-slow” traditional open-sources intelligence collection and tradecraft techniques are force-multipliers in successful exams. In the rush to get on the target, engagement preparation and thorough reconnaissance often become abbreviated. Missed intelligence often leads to prolonged engagement timelines, susceptibility to cognitive biases, missed opportunities, attack deceleration, and an over-reliance on automated tooling logic.

SPECIAL AGENT JASON PEARSON and SPECIAL AGENT KEITH MULARSKI
Topic: "What keeps me up at night..."
Abstract
A discussion of Botnets, Malware, Cyber Crime & the Criminal Underground

DOUGLAS BROWN
Topic: Information Assurance, an IT Audit Perspective.
Abstract:
Auditing as it relates to information assurance.

Network Security Monitoring: An Open Community Approach

IUP- Information Assurance Day, 2011

Greg Porter
11/10/11

ALLEGHENY DIGITAL

Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

Introduction

- Greg Porter
- Working in the field, ~ 10 years
  - Vulnerability Assessments
  - Penetration Testing
  - Incident Response
  - Security Governance
- Primarily “Big 4” consulting
- Visiting Scientist, SEI-CERT
- Founder, Allegheny Digital

This Presentation

- Based on technical and non-technical security assessment activities and direct observations made over the past several years
- Lack of reasonable network security monitoring in many organizations is…*rather pervasive*
- Intent is to provide an overview of some promising "open community" platforms

Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

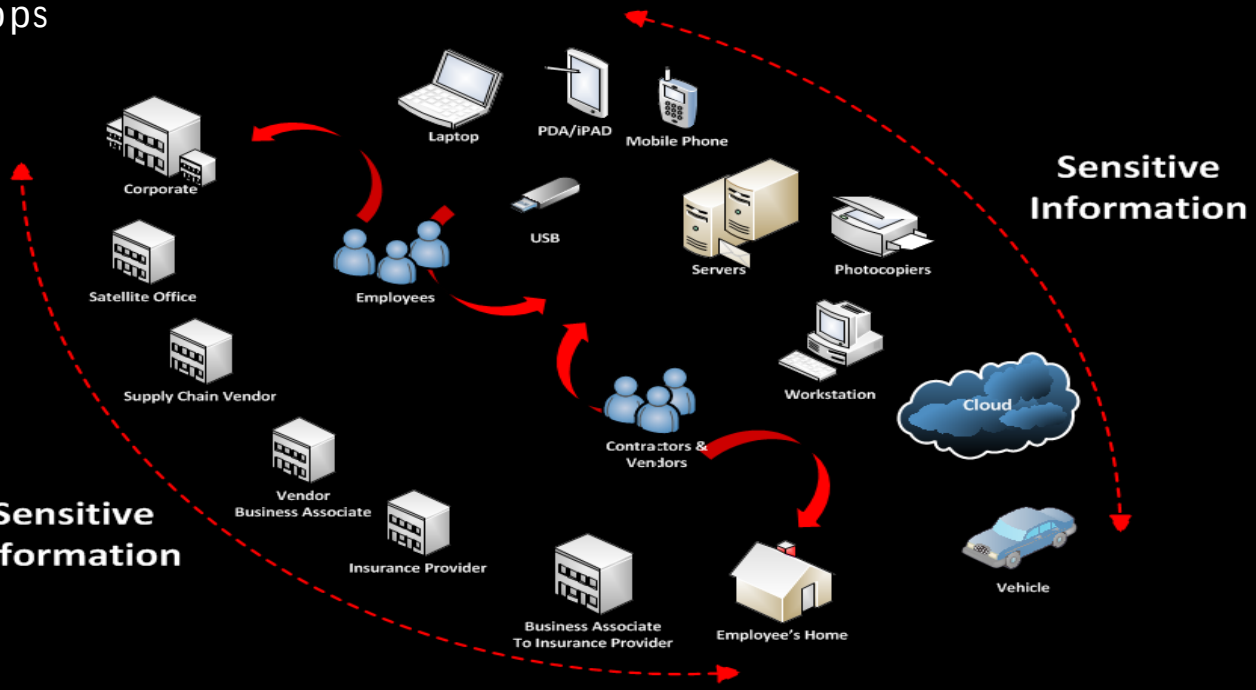
Current State

- Where are we today?
- The proliferation of malware isn't slowing
- 2010 the biggest year ever for total malware production
  - At least 20 million new pieces of malware last year alone
- 55,000 new instances of malware/day[1]
- *There is now more malicious code being created today, worldwide, than there is legitimate software*[2]

1. Source: McAfee
2. Source: Symantec

The Unbounded Enterprise

- Data Anywhere ≠ Data Everywhere
- More endpoints, more mobile devices add to the challenge of protecting sensitive information
  - A general lack of security awareness among end users
  - Limited offerings and maturity of mobile safeguards, widespread non-secure apps



Every Business is a Target

- Even seemingly "well defended" organizations are getting compromised
- The past 24 months have seen the likes of Google, RSA, AT&T, IBM, Northrop Grumman, and numerous others fall to targeted cyber attacks
- How do many successful businesses often find out they've had a breach of sensitive information?
- Does your company have the necessary network visibility to detect and mitigate potential risks before they occur?

What's Changed?

- Attacks are increasing at an exponential rate
- This is contrary to what many people think because the attackers have changed how they operate
  - (Past) Visible → Stealthy (Today)
  - (Past) Disruptive → Data driven (Today)
  - (Past) Low hanging fruit → Targeted (Today)
  - (Past) Static → Dynamic (Today)
  - (Past) Ad hoc → Persistent (Today)
  - (Past) Basic → Advanced (Not an absolute)

Source: Dr. Eric Cole

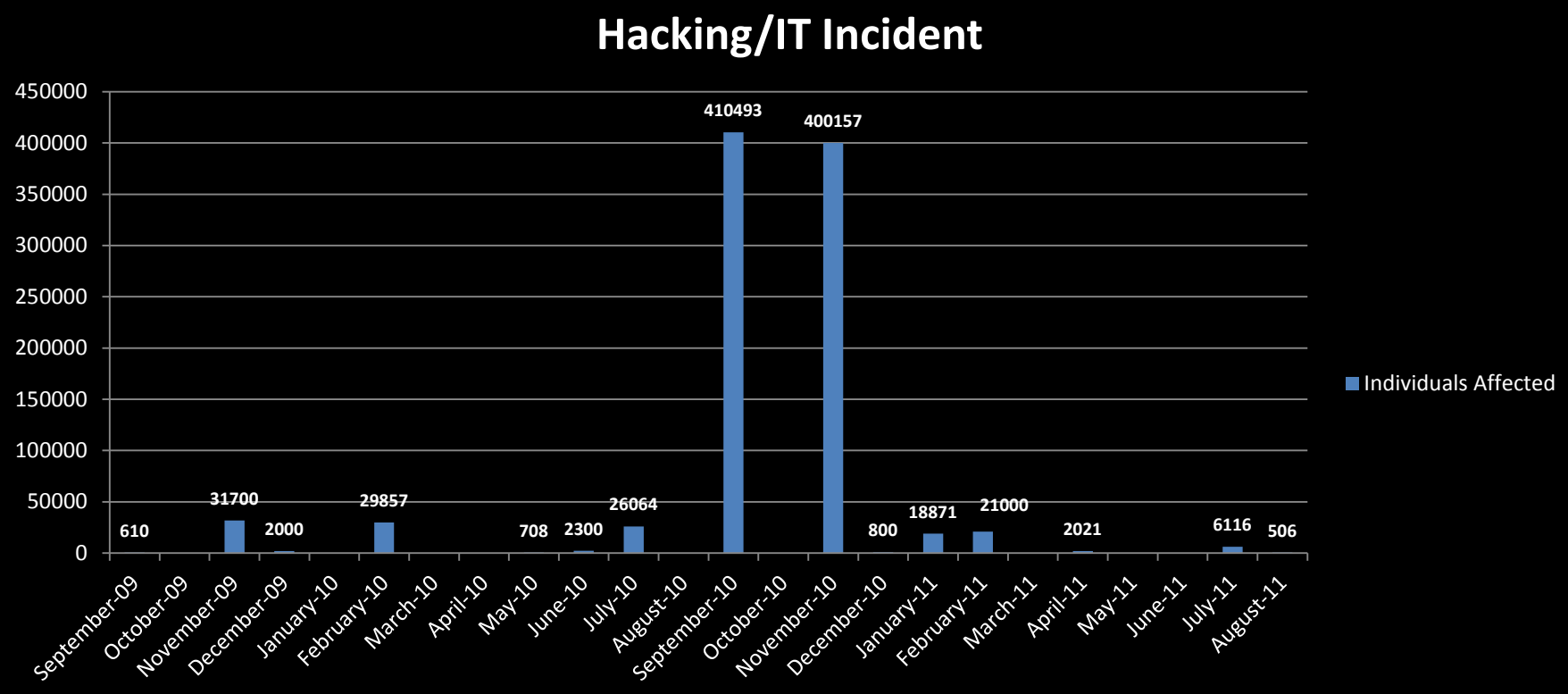
Your Information @ Stake

- Healthcare: NEA Baptist Clinic
  - 3,116 affected
  - Clinic's web site compromised, usernames, passwords, and in some cases additional details
- Retail: Adidas
  - 500,000
  - Website compromised, email addresses and passwords dumped by hacker
- Education: Florida International University
  - 19,500
  - Emoticon discovered in internal database suggested that database with 19,500 students' names, dates of birth, Social Security numbers, and GPAs might have been accessed by hacker
- Government: BART Police Officer Association
  - Hackers released the private data of more than 100 BART police officers
  - Disclosure of 2,000 usernames and passwords by the hacking collective Anonymous against a San Francisco transportation website

Source: http://datalossdb.org

An Anecdote? Healthcare & Breaches

- As required by the HITECH Act, the Secretary of HHS must post a list of breaches of unsecured protected health information (PHI) affecting 500 or more individuals.



Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Agenda

- Introduction
- Current State
- NSM & Open Community Options
- Conclusion

Network Security Monitoring

- Preventative measures will eventually fail…some intruders are smarter, more patient than you
- NSM is the collection, analysis, and escalation of indications and warnings (I&W) to detect and respond to intrusions
- An IDS alert provides a potential indicator that of a security related event
- IDS != NSM
- Prepare for an incident before it occurs, collect as much as you technically and legally can

Source: Richard Bejtlich

Network Security Monitoring – ii

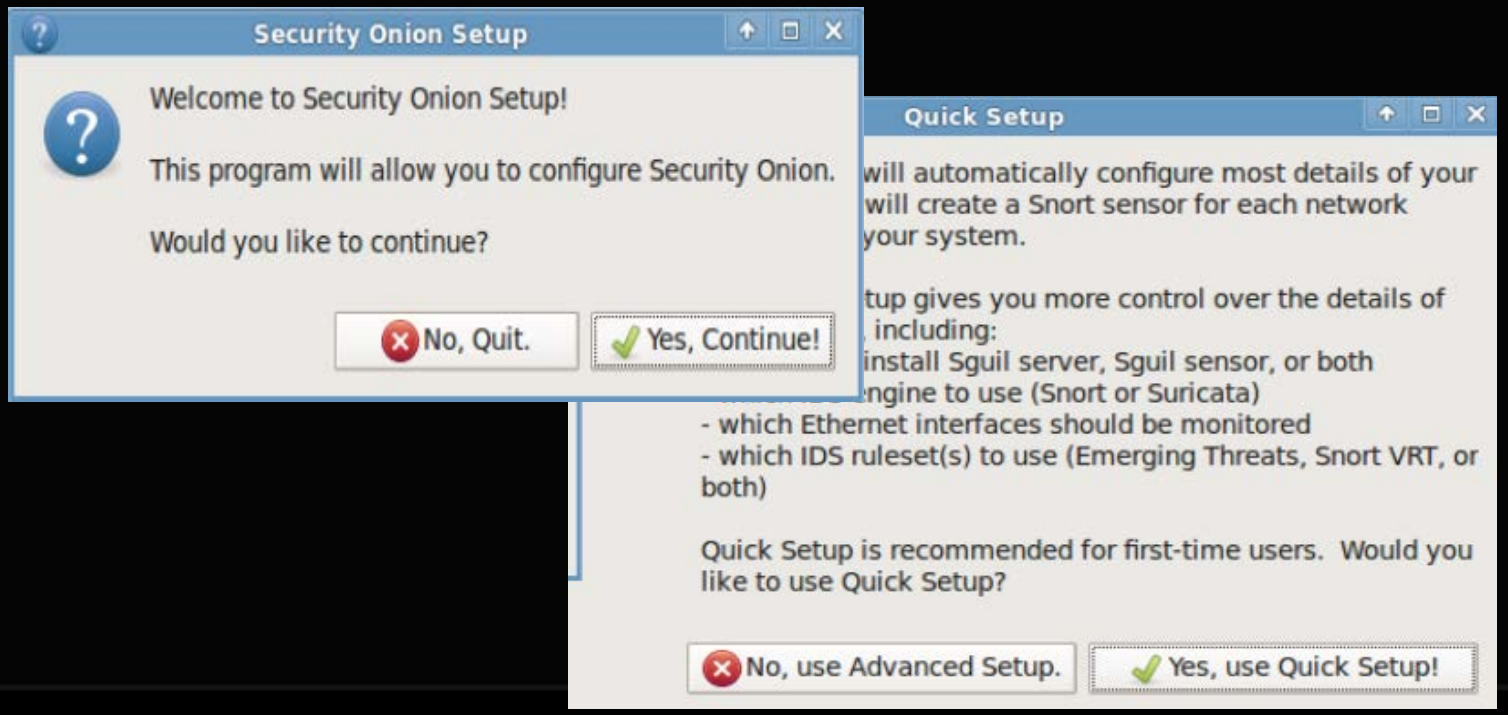
- Regarding data collection
  - Storage costs are decreasing
  - Data sampling and traffic analysis is better than doing nothing
- NSM provides needed context to make intelligent decisions
  - *Alert* data provides a potential indicator of security incidents
  - *Session* data is a content neutral summary of transactions
  - *Full content* data captures packet-level details, including application content
  - *Statistical* data summarizes traffic

Security Onion

- A Linux distro developed by Doug Burks
- Excellent resource for IDS and NSM
  - Available at http://securityonion.blogspot.com/
- Contains a breadth of NSM tools
  - Snort, Suricata, Sguil, Wireshark, Squert, etc.
- Sguil is the de facto reference implementation of NSM
  - Alert data (NIDS alerts from Snort/Suricata *and* HIDS alerts from OSSEC)
  - Session data (Security Analyst Network Connection Profiler SANCP)
  - Transaction data (HTTP logs from httpry)
  - Full content data (daemonlogger)

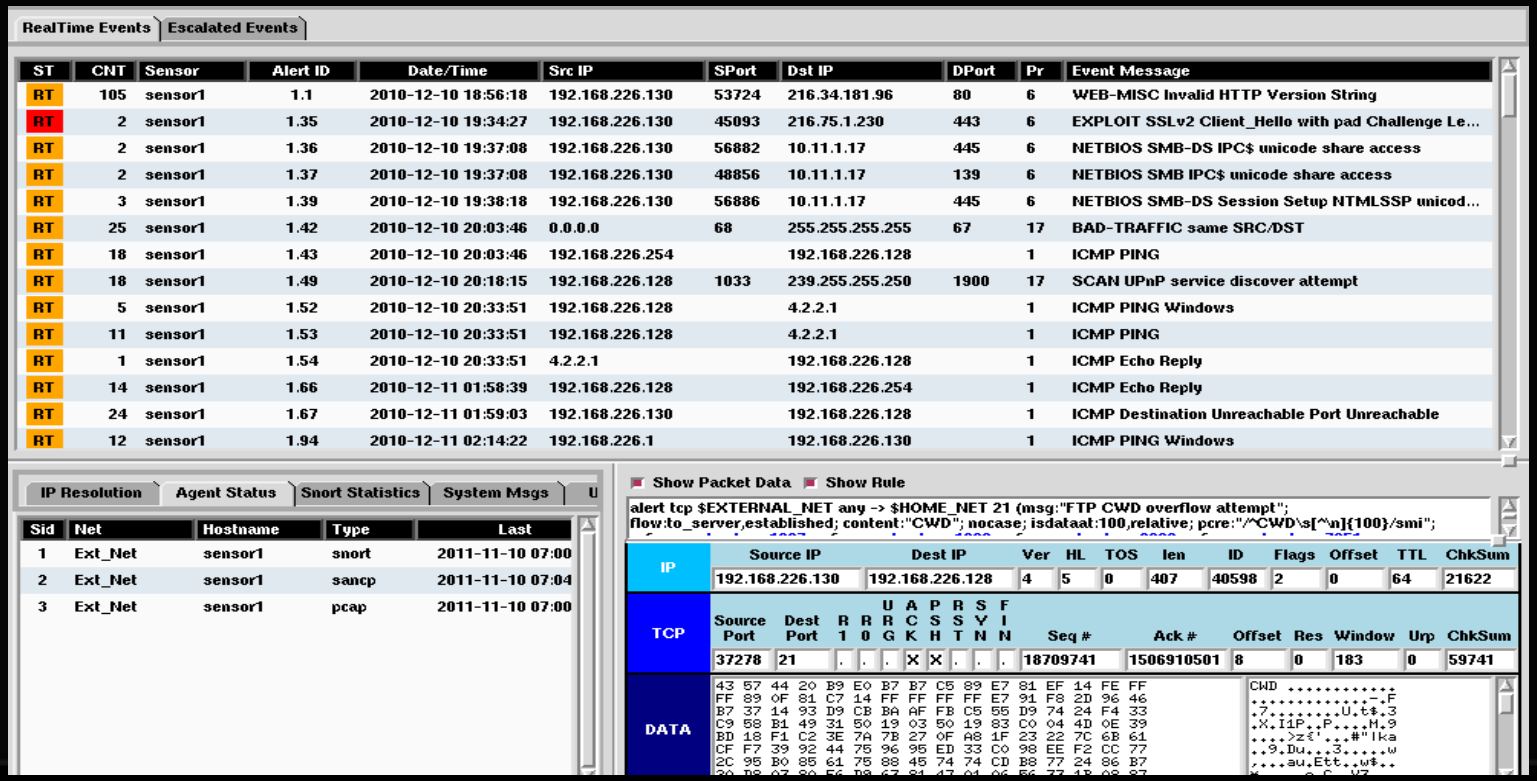
Security Onion -ii

- SO's Quick Setup feature will automatically configure the essential details of your system, creating a Snort sensor for each network interface on your system



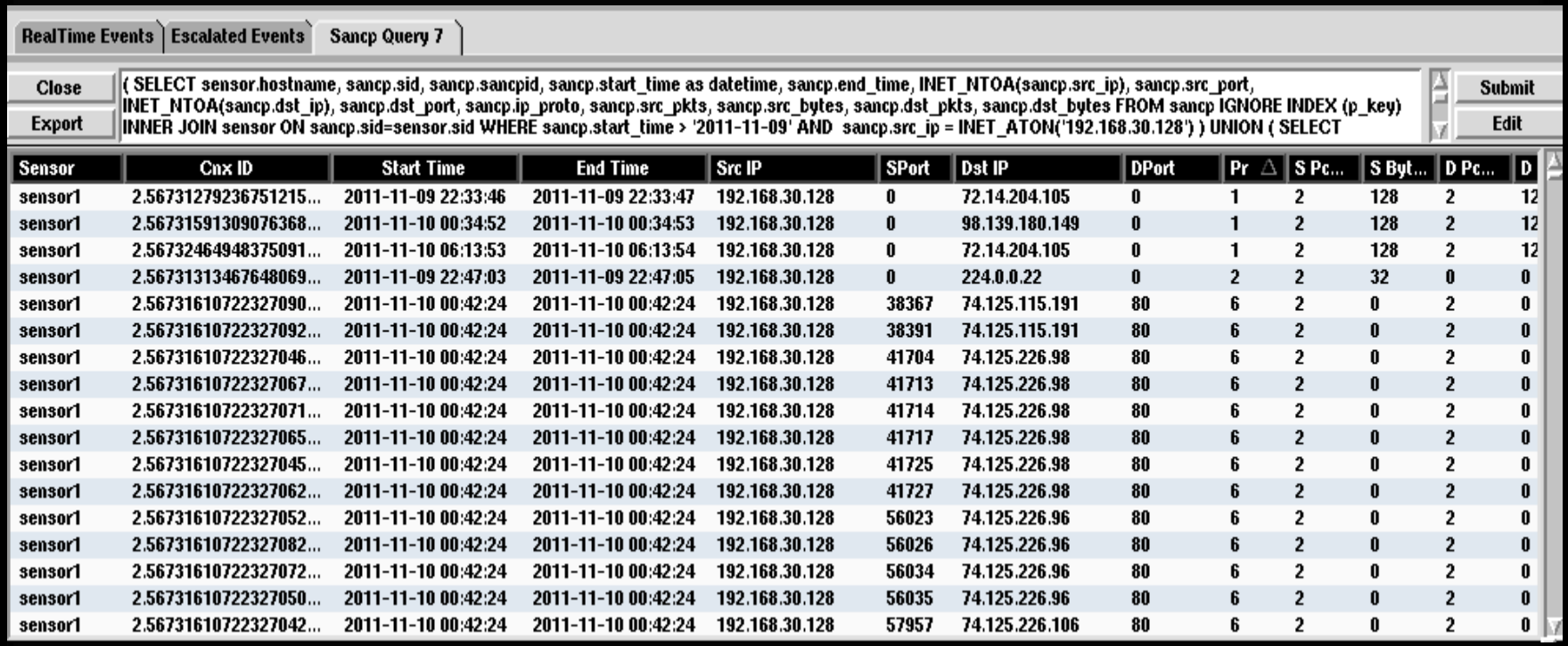
Security Onion -Sguil

- Sguil's interface provides the analyst with the ability to contextualize network traffic via Alert, Session, Full Content, and/or Statistical Data



Security Onion -iv

- Utilizing Squil to view session data



RealTime Events | Escalated Events | Sancp Query 7

Close / Export

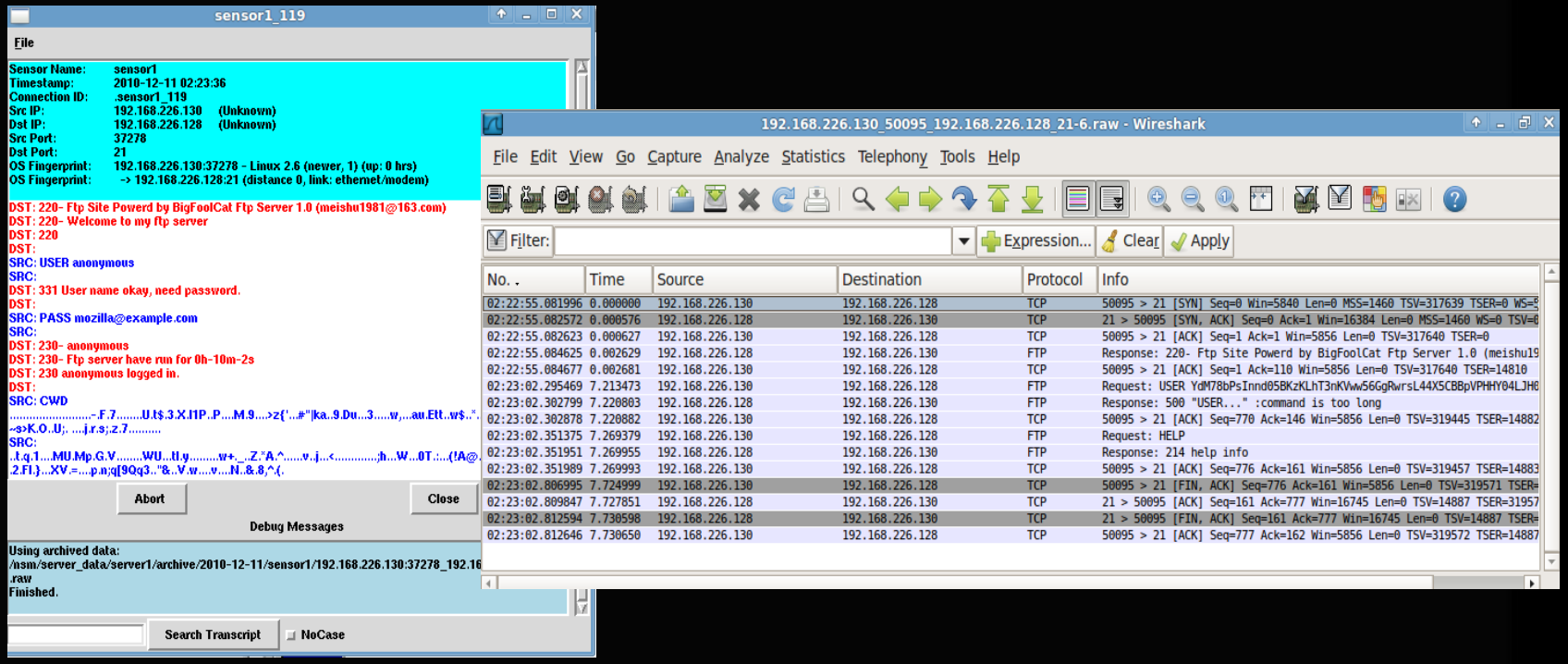
```
( SELECT sensor.hostname, sancp.sid, sancp.sancpid, sancp.start_time as datetime, sancp.end_time, INET_NTOA(sancp.src_ip), sancp.src_port,
INET_NTOA(sancp.dst_ip), sancp.dst_port, sancp.ip_proto, sancp.src_pkts, sancp.src_bytes, sancp.dst_pkts, sancp.dst_bytes FROM sancp IGNORE INDEX (p_key)
INNER JOIN sensor ON sancp.sid=sensor.sid WHERE sancp.start_time > '2011-11-09' AND  sancp.src_ip = INET_ATON('192.168.30.128') ) UNION ( SELECT
```

Submit / Edit

Sensor	Cnx ID	Start Time	End Time	Src IP	SPort	Dst IP	DPort	Pr △	S Pc...	S Byt...	D Pc...	D
sensor1	2.56731279236751215...	2011-11-09 22:33:46	2011-11-09 22:33:47	192.168.30.128	0	72.14.204.105	0	1	2	128	2	12
sensor1	2.56731591309076368...	2011-11-10 00:34:52	2011-11-10 00:34:53	192.168.30.128	0	98.139.180.149	0	1	2	128	2	12
sensor1	2.56732464948375091...	2011-11-10 06:13:53	2011-11-10 06:13:54	192.168.30.128	0	72.14.204.105	0	1	2	128	2	12
sensor1	2.56731313467648069...	2011-11-09 22:47:03	2011-11-09 22:47:05	192.168.30.128	0	224.0.0.22	0	2	2	32	0	0
sensor1	2.56731610722327090...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	38367	74.125.115.191	80	6	2	0	2	0
sensor1	2.56731610722327092...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	38391	74.125.115.191	80	6	2	0	2	0
sensor1	2.56731610722327046...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41704	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327067...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41713	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327071...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41714	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327065...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41717	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327045...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41725	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327062...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	41727	74.125.226.98	80	6	2	0	2	0
sensor1	2.56731610722327052...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	56023	74.125.226.96	80	6	2	0	2	0
sensor1	2.56731610722327082...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	56026	74.125.226.96	80	6	2	0	2	0
sensor1	2.56731610722327072...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	56034	74.125.226.96	80	6	2	0	2	0
sensor1	2.56731610722327050...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	56035	74.125.226.96	80	6	2	0	2	0
sensor1	2.56731610722327042...	2011-11-10 00:42:24	2011-11-10 00:42:24	192.168.30.128	57957	74.125.226.106	80	6	2	0	2	0

Security Onion -ii

- Squil can render full content data via its transcript function or by calling Wireshark



Session Data With NetFlow

- NetFlow is a traffic-summarization format that was first implemented by Cisco Systems and other router manufacturing companies, primarily for billing purposes
- Some of the NetFlow standard fields
  - source address, destination address
  - source port, destination port
  - protocol
  - bytes, packets
  - TCP flags
  - start time, duration
  - end time
  - sensor identification

Session Data With NetFlow ii

- Sample flow data

SEI/CERT - SiLK

```
            sIP|            dIP|sPort|dPort|pkt|bytes|flags|
63.236.206.174|   72.24.144.5|44800|   25|  21|19606|FS PA|
   72.24.144.5|63.236.206.174|   25|44800|  17| 1066|FS PA|
63.236.206.174|   72.24.144.5|44800|   25|   1|   40|   R |
63.236.206.174|   72.24.144.5|44800|   25|   1|   40|   R |
63.236.206.174|   72.24.144.5|44800|   25|   1|   40|   R |
63.236.206.174|  72.24.146.90|44800|   25|   1|   40|   R |
  72.24.146.90|63.236.206.174|   25|44800|   1|   49| F PA|
~
~
~
~
~
~
~
~
"WhatIsThis-1.txt" 9L, 473C                   9,0-1         All
```

Session Data With NetFlow iii

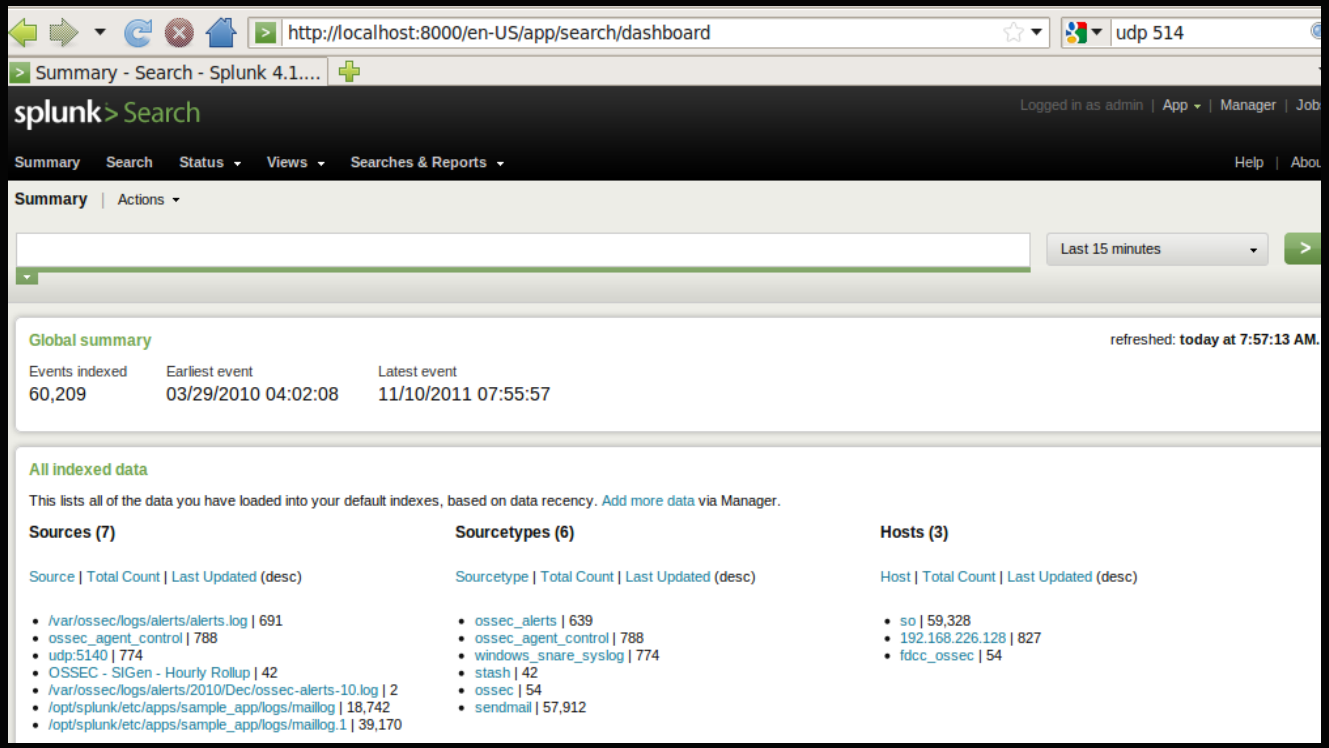
- Tools such as fprobe, and flow-tools can help

SEI/CERT - SiLK

```
            sIP|           dIP|pro|pkts|bytes|       sTime|
66.142.134.179|72.24.150.186|  1|    2|  122|00:00:00.582|
66.142.134.179|72.24.148.123|  1|    2|  122|00:00:00.911|
66.142.134.179| 72.24.146.95|  1|    2|  122|00:00:01.783|
66.142.134.179|72.24.159.123|  1|    2|  122|00:00:01.895|
66.142.134.179|72.24.145.227|  1|    2|  122|00:00:02.220|
66.142.134.179| 72.24.154.87|  1|    2|  122|00:00:02.329|
66.142.134.179|72.24.149.212|  1|    2|  122|00:00:02.550|
66.142.134.179| 72.24.158.18|  1|    2|  122|00:00:02.766|
66.142.134.179| 72.24.150.34|  1|    2|  122|00:00:02.875|
66.142.134.179|72.24.153.102|  1|    2|  122|00:00:02.879|
66.142.134.179| 72.24.144.61|  1|    2|  122|00:00:03.421|
66.142.134.179|  72.24.129.2|  1|    2|  122|00:00:03.530|
66.142.134.179|72.24.129.224|  1|    2|  122|00:00:03.642|
66.142.134.179|72.24.151.196|  1|    2|  122|00:00:04.184|
~
"WhatIsThis-2.txt" 15L, 871C                  15,1          All
```

Log Analysis

- Splunk, collects and indexes machine data, such as logging data
- Free to download



Agenda

- Introduction
- Current State
- Defensive Strategies
- Conclusion

Conclusion

- NSM uses an alert as the beginning of the investigative process, not the conclusion
  - Assists the analyst in establishing network situation awareness to track and suppress intrusions
- Data breaches are costing businesses millions of dollars
- Don't let a customer be your first notification that something is amiss within your current data protection and compliance program
- NSM can be initiated
- It is the responsibility of assigned organizational management to take reasonable and appropriate measures to safeguard sensitive information in line with regulatory demands and consumer expectations

Resources

- Security Onion
  - http://securityonion.blogspot.com/
- Richard Bejtlich
  - "The Tao of Network Security Monitoring"
- CERT
  - http://www.cert.org
- Forum of Incident Response & Security Teams ("FIRST")
  - http://www.first.org

Questions?

> there is no secure end-state - only constant vigilance

THANK YOU!

www.alleghenydigital.com

1.877.234.0001

ALLEGHENY DIGITAL

- Professional Services
  - Information Security Consulting
  - Managed Services
  - Training & Education
- Breadth of Experience
  - Healthcare
  - Manufacturing
  - Technology
  - Education
  - Finance
  - Energy
- Western PA based

Red Teaming Approaches, Rationales, Engagement Risks and Methodologies

Indiana University of Pennsylvania
Information Assurance Day 2011
Session 3: 11-12 noon
IUP HUB Delaware Room

d/b/a Mark Yanalitis

Goals for today

- Define Red Teaming and its' rationale
- Discuss differences between commercial and full-spectrum Red Teaming
- Discuss differences between commercial and full-spectrum methodologies
- Examine common engagement risks
- Application of Red Teaming methods
- A companion document exists as supplemental reading resource for this presentation

Red Teaming Definitions

"An array of activity where the overall goal is to understand the adversaries perspective in order to identify one's own vulnerabilities and challenge one 's own assumptions."[1]

"Authorized, adversary-based assessment for defensive purposes."[2]

"Review of control design and threat-based penetration testing to simulate actual attacks."[3]

Commercial v. Full Spectrum

Lets explore the motivating factors for commercial and full-spectrum red teams

Commercial engagements

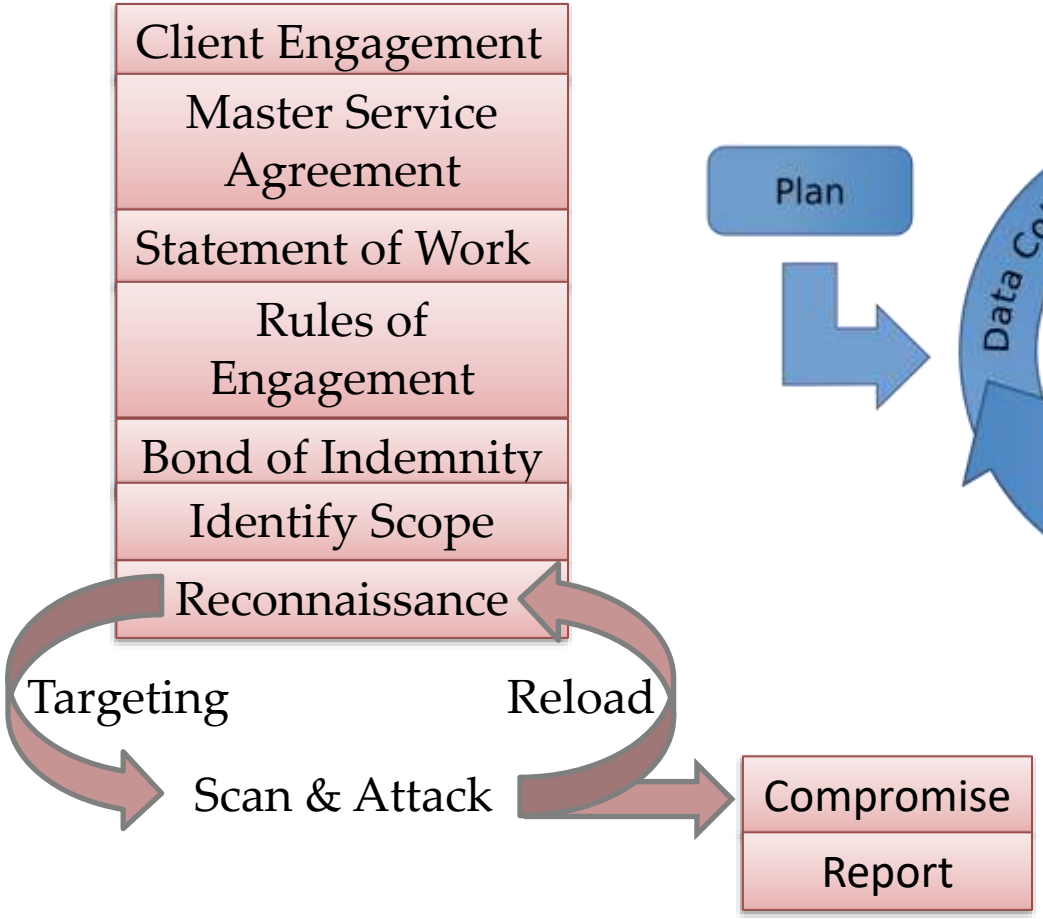
- Threat-based modeling
- Compliance mandates
- IT Audit adjunct testing
- Goal is quick penetration
- Cost and time driven
- Automation dependency
- Survey the known

Full-Spectrum engagements

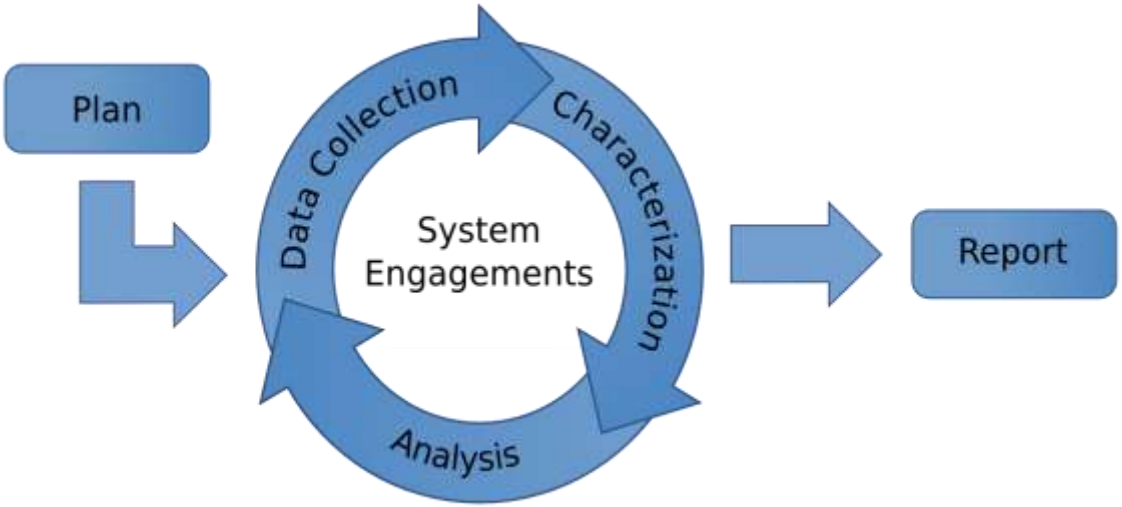
- Capabilities-based or hybrid modeling
- Simulations
- Goal is understanding
- Risk analysis driven
- Human in the loop
- Expand the knowable by parsing the unknown

Methodologies

Commercial

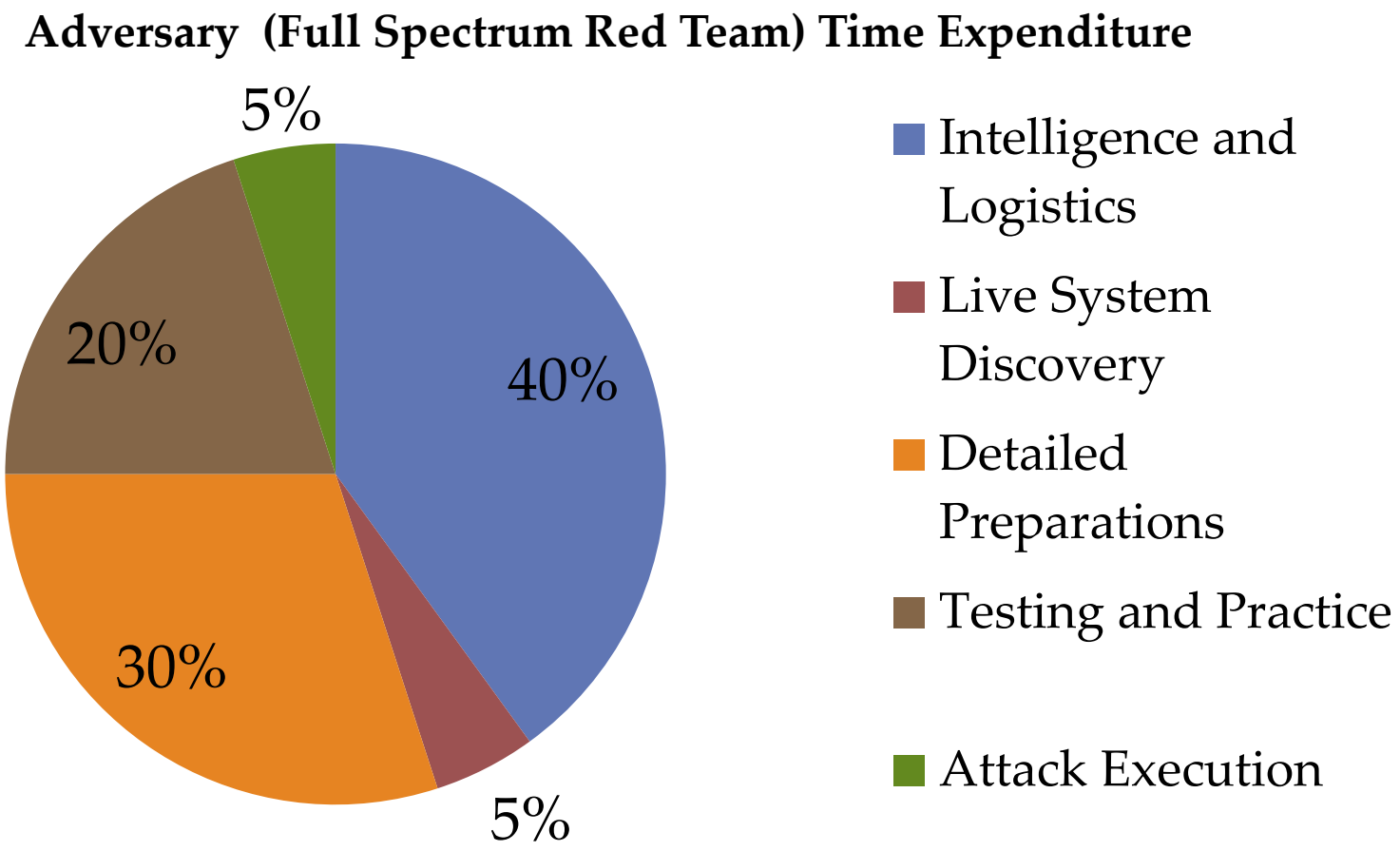


Full Spectrum



Source: Sandia National Laboratories IDART, 2011

The Intelligence Process

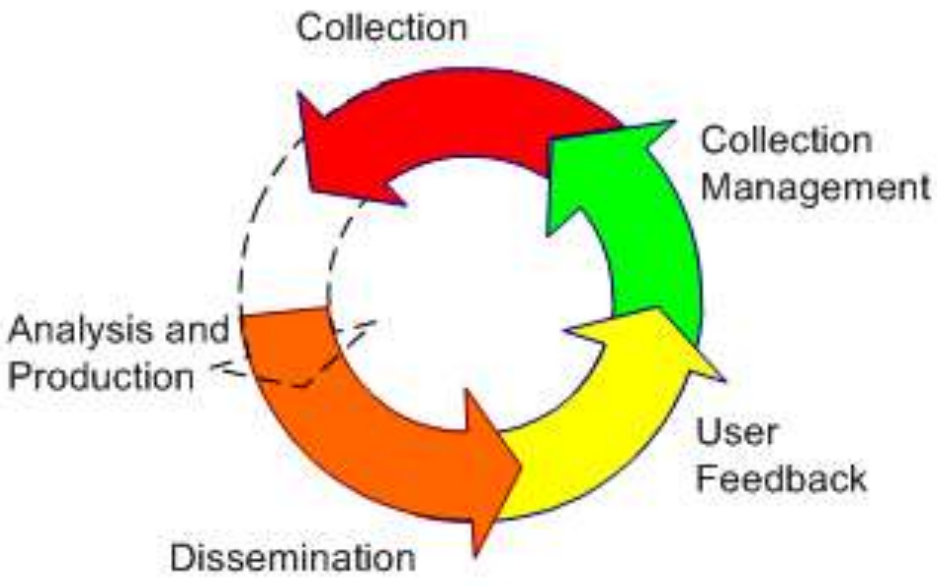


[4] Schudel, G. and Wood, B. (RAND, SANDIA & GTE: 2000)

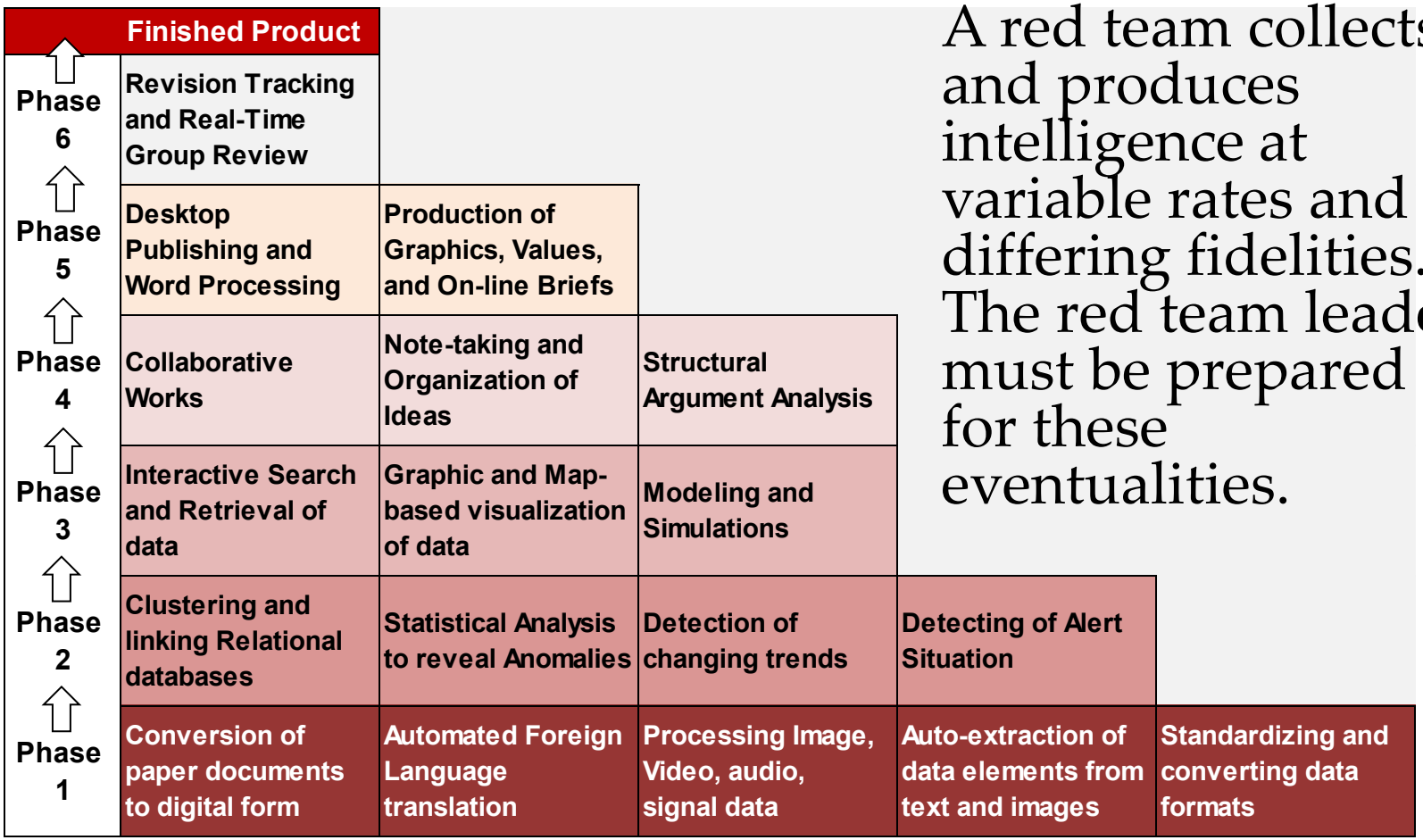
Intelligence Cycle

A full-spectrum red team will focus upon likely adversarial courses of action as well as current capabilities.

Internally to the team, a need exists to have common doctrinal understanding of resource identification, intelligence collection, collection management, training, and leadership.



Intel Fusion Approach



A red team collects and produces intelligence at variable rates and differing fidelities. The red team leader must be prepared for these eventualities.

[5] Adapted from Steele, Robert, D. (New Craft of Intelligence: 2002)

Bias in the Intel process

Sources of cognitive error

Sources of cognitive error can be found in individual minds, the collective agreement of the team, team composition, and in the quality of support given to the effort. Each individual team member carries both a cognitive bias as the known outsider pre-judged by their own past experiences, as well as the bias of their culture.

Organizational and environmental bias indicators

The assignment is not taken seriously

The team or sponsor becomes too removed from the decision-making process

A lack of interaction with the blue team

Insufficient access to the details of the target

Loss of team confidences

The team fails to capture the details of the adversary, and instead mirrors itself

The red team does offers no challenge to the blue team

Thin top cover: the lack of a robust channel to act on findings in a timely manner, or consider findings with any seriousness.

Applied post-event after many bodies already have been thrown at the problem

The wrong team targeting the wrong problem (Threat-based team vs. a capabilities based problem)

A lack of clarity on the urgency of issues at hand

The red team approach is a one-time activity

[6] Defense Science Board. *Task Force Report on The Role and Status of Red Teaming Activities*: (DoD: 2003)

Role play the Adversary

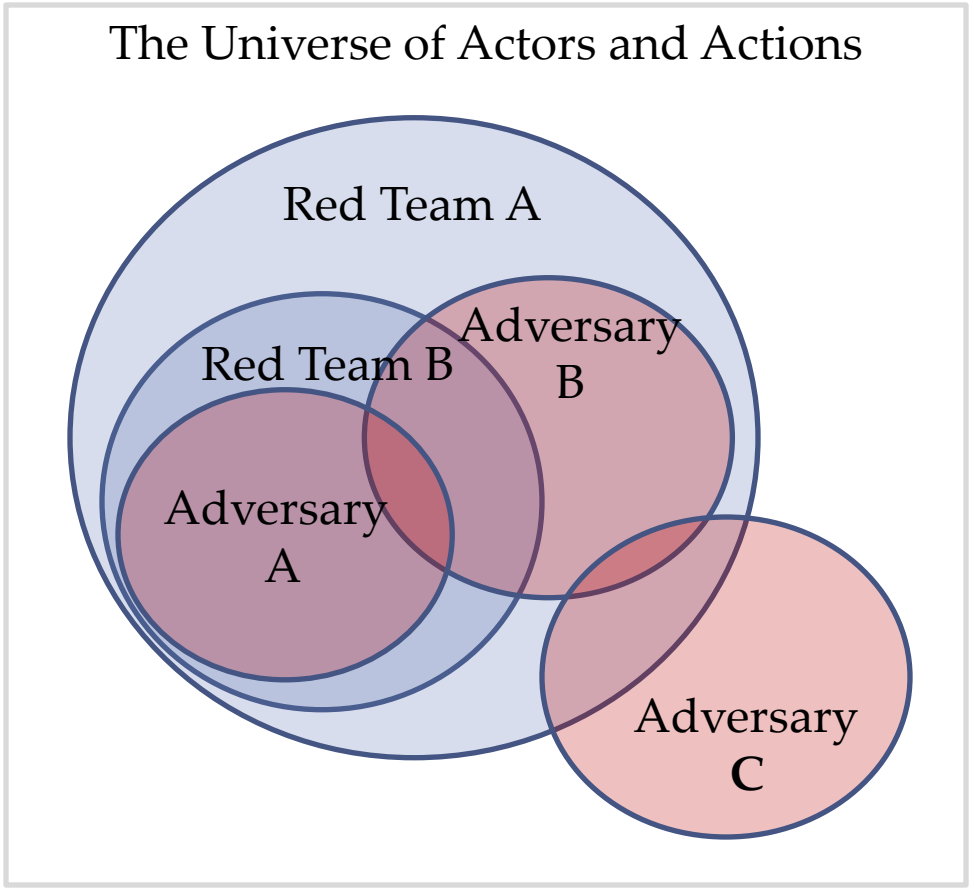
Lets explore the difference between a threat-based adversary model and capabilities-based adversary model.

Threat – A threat represents a known quantity, a known effect singular in origin, essentially a Pathogen-Antigen model. A threat is an X-Y direct, or inverse relationship.

Capability – Actors (or a confederation of multiple actors) capable of achieving a singular goal either due to access to resources, or some form of institutional support. The force multiplier effects of capability-based actors behave like an algebraic expression where leading factors have orders of magnitude, possibly even having orders of operation.

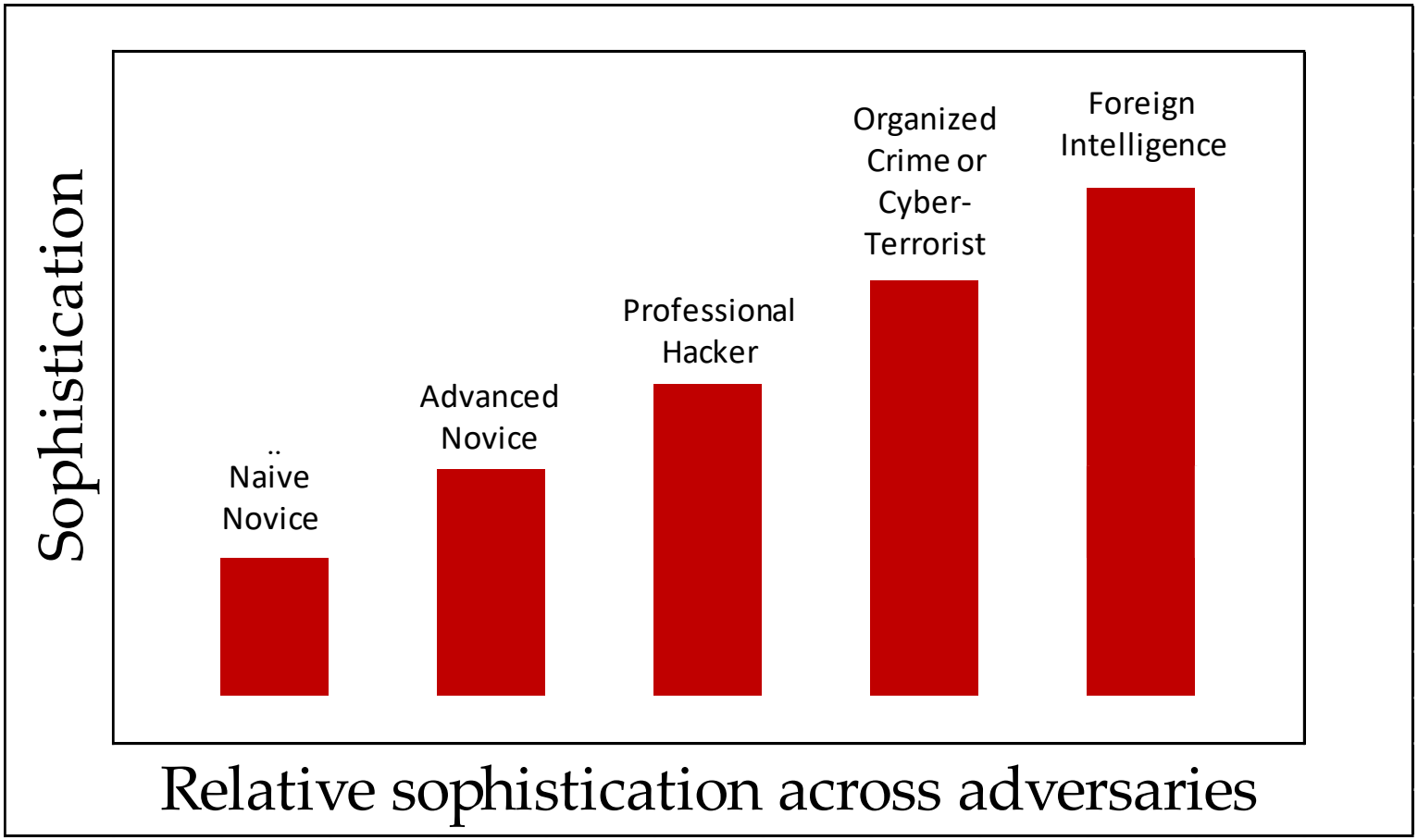
Adversarial Modeling

In the full-spectrum Red Team context, the sponsor may need more than one type of red team to realistically model the capability. In the commercial world, modeling capability-based actors is the exception, not the norm.



Source: Sandia National Laboratories IDART, 2011

Adversarial Prototyping



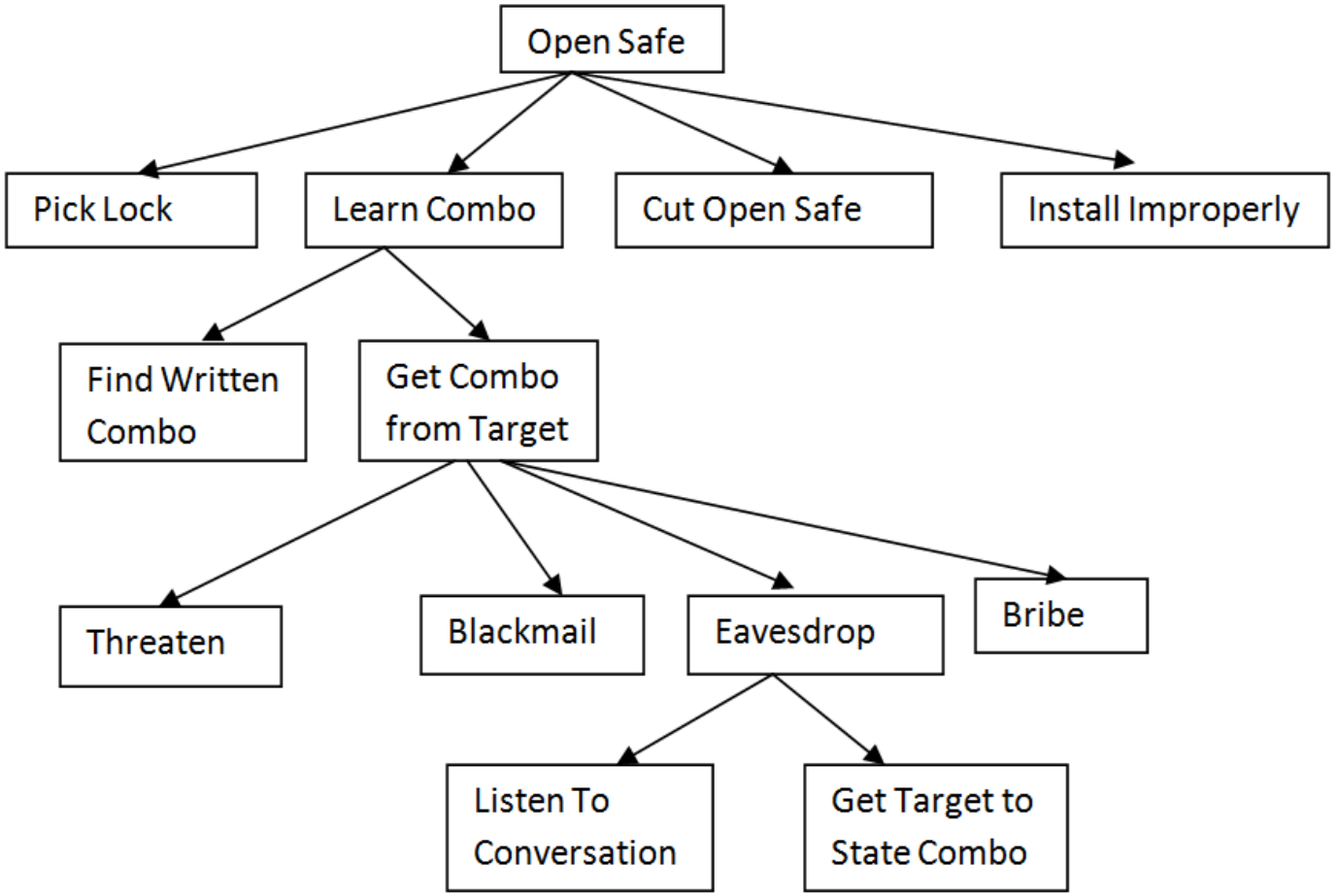
[7] *Op. Cit.* Schudel, G. and Wood, B. : 2000

Threat Profiling

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE CYBER	KNOWLEDGE KINETIC	ACCESS
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

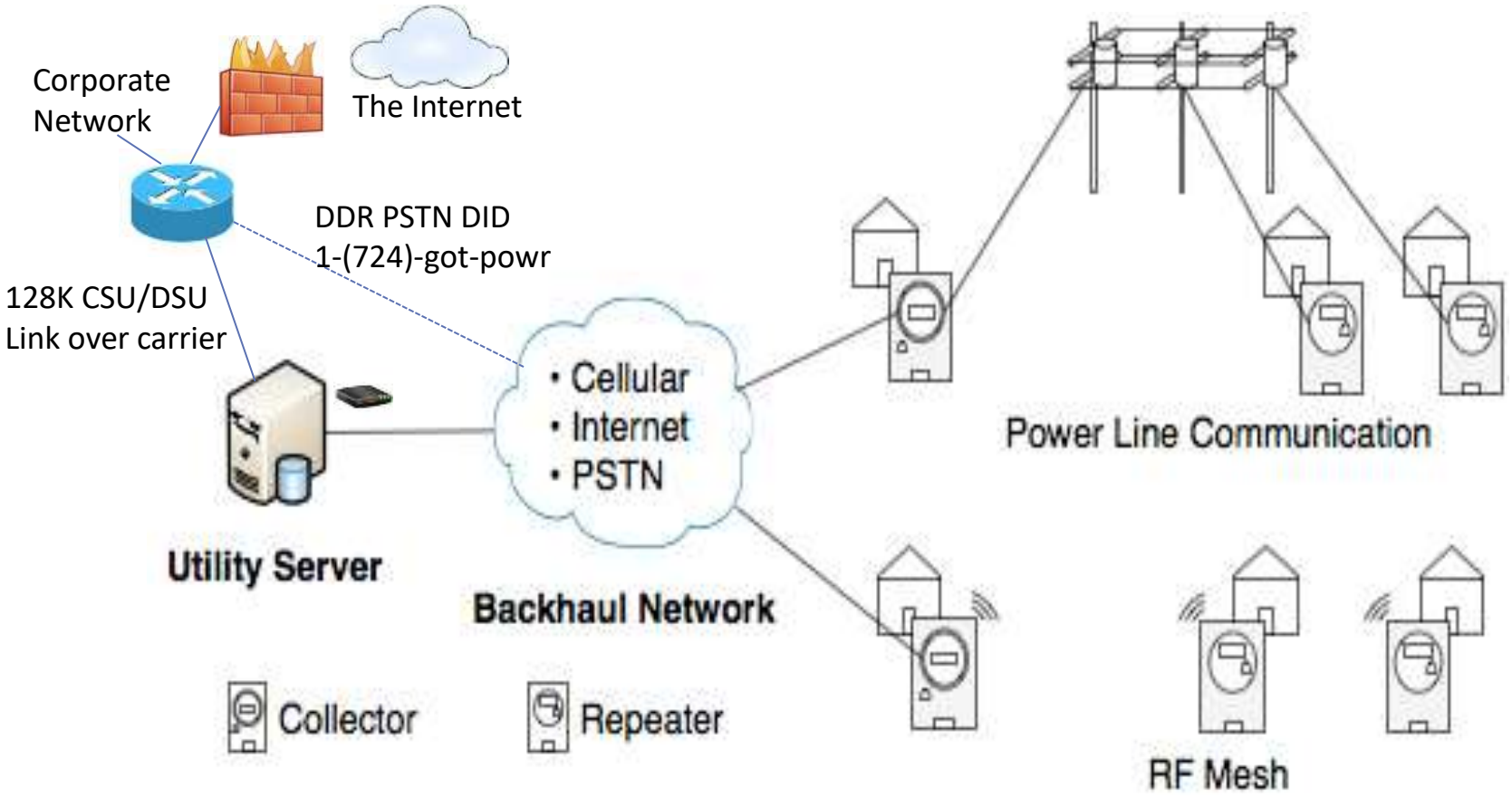
[8] Duggan, *et. al.* SANDIA, 2007

Attack Trees



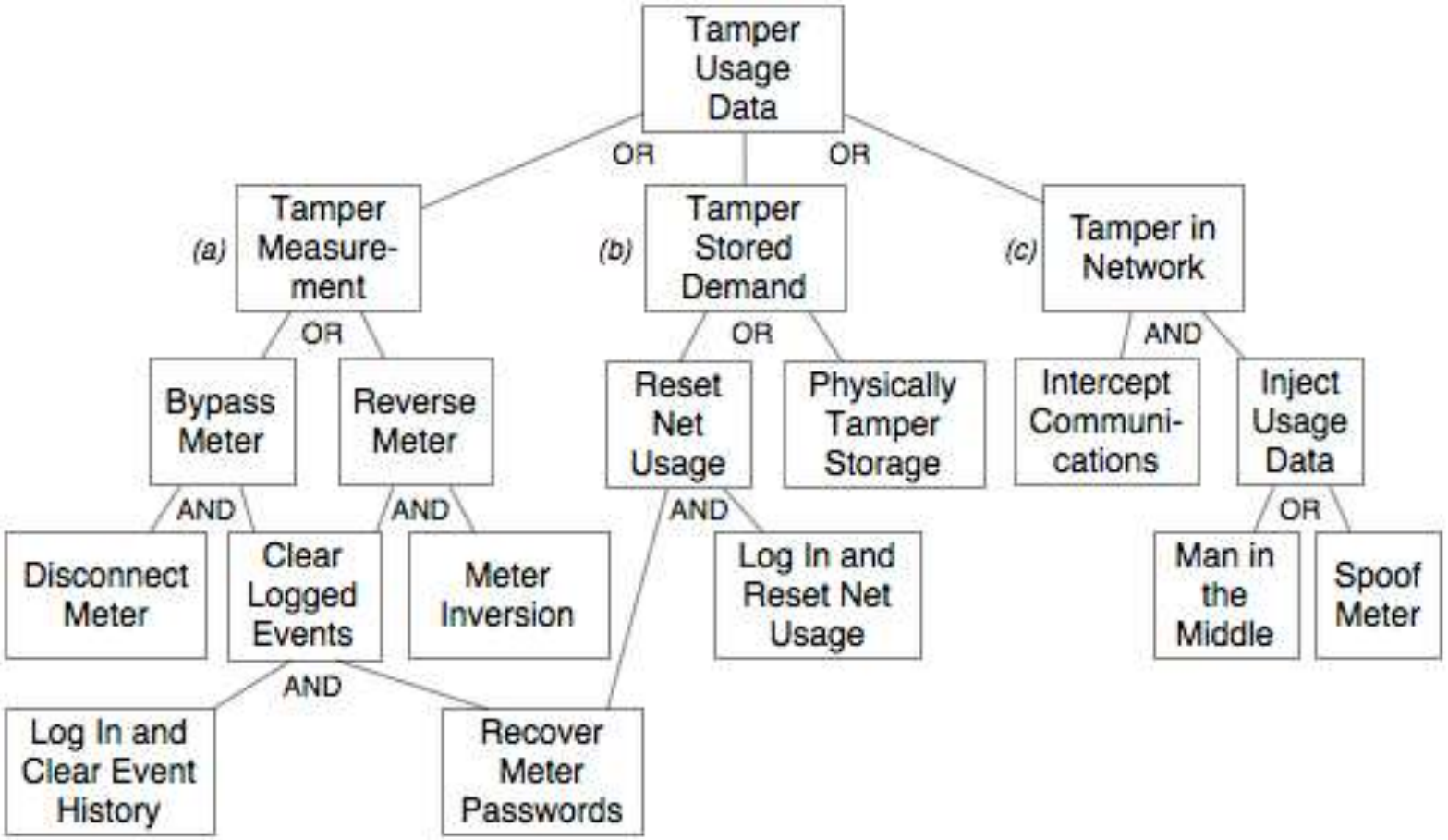
[9] Schneier, Bruce. *Modeling Security Threats* (Dr. Dobb's Journal: 1999)

Smart Grid Attack Diagram



[10] Penn State University SIIS Laboratory. (Network and Security Research Center: 2010)

Smart Grid Attack Tree



[11] *Ibid*. Penn State University SIIS Laboratory: 2010

When to Use Red Teaming

Don't use RT methods for,	Do use RT methods for,
Simple systems or processes	Complex systems or complex system of systems
Undefined environments	Hostile and well-defined environments
Low consequence systems	System with unknown consequences
Problems already identified	Adaptable adversaries
Compliance and certification suffices	Informing on security trade-offs
When unready to receive an extreme answer	Training and doctrine

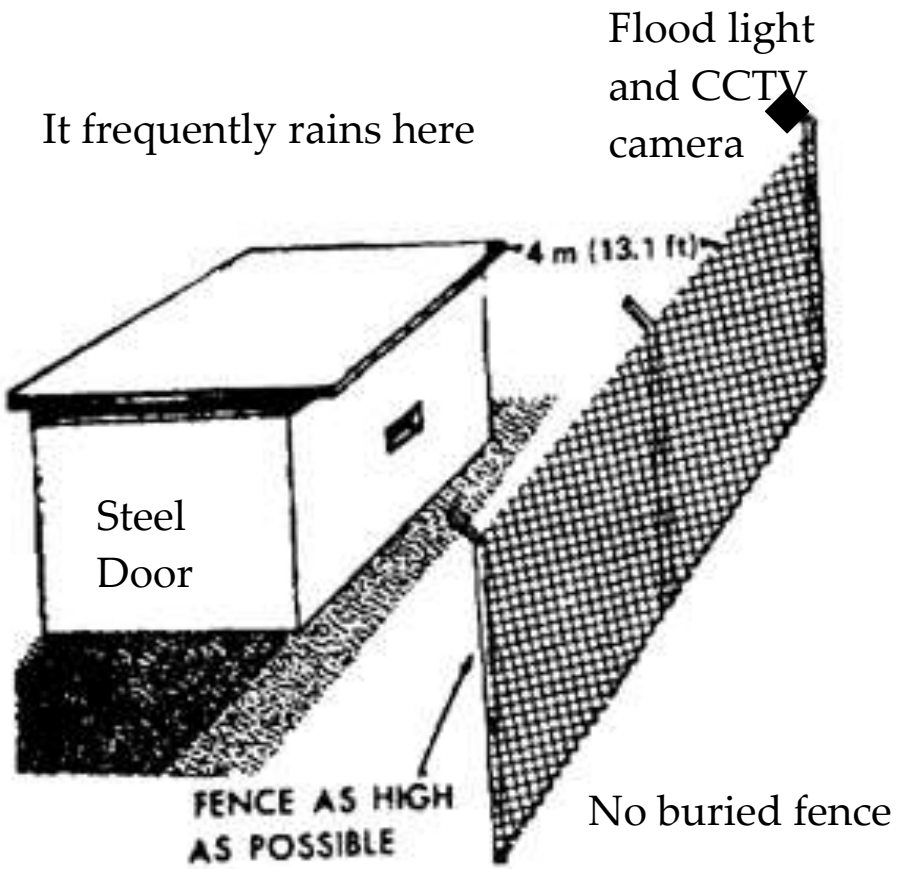
[12] Atkins, William. *Read Teaming – It's Good to be Bad.* (Missouri S&T ACM SIG in Security: 2010)

Ok, you try it now.

Target: A reciprocating high-speed gas compressor

Source: BPI Compression 2011

The red team simulation revealed complete destruction of the compressor and block house site plan in 10 minutes. What was the solution? Where are the vulnerabilities? why did the solution work?



½ ton pickup

A cinderblock

Fender Jack

Stump Remover

Mentos

Duct Tape

Magnesium Ribbon

2 black Super Fan Suits

Five 2L bottles of Cola

One 2L bottle of Clorox

1 Sling Shot

Estimated 3 weeks of site observation and rehearsal

Use your powers for the greater good, not evil.

References

1 McGannon, Michael. *Developing Red Team Tactics, Techniques, and Procedures.* (Red Team Journal: APR 2004). Internet. Found at http://redteamjournal.com/

2 Sandia IDART Methodology. http://idart.sandia.gov/methodology/index.html

3 Price Waterhouse Coopers. *Is your critical infrastructure safe?* (PWC LLP:2010) Internet. Found at http://www.pwc.com/en_US/us/industry/utilities/assets/cyber-attacks.pdf 5.

4 Schudel, G. and Wood, B. *Modeling the Behavior of a Cyber Terrorist*. (RAND National Security Research Division proceeding of workshop. Appendix C: Santa Monica, California: 2000) 49-59. Internet. Found at http://www.csl.sri.com/users/bjwood/cyber_terrorist_model_v4a.pdf.

5 Steele, Robert, D. *The New Craft of Intelligence: Achieving Asymmetric Advantage in the Face of Nontraditional Threats*. (U.S. Army War College Strategic Studies Institute: 2002). 34-36.

6 Department of Defense Science Board. *Task Force Report on The Role and Status of Red Teaming Activities* (Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Washington, D.C. 20301-3140:2003). Internet. Found at *www.au.af.mil/au/awc/awcgate/dod/dsb-redteam.pdf*

7 *Op. Cit.* Schudel and Wood, 2000.

8 Duggan, David, P., Thomas, Sherry R., and Veitch, Cynthia K.K., and Woodward, Laura. *Categorizing Threat - Building and Using a Generic Threat Matrix*. (SANDIA National Laboratories, Albuquerque NM. REPORT SAND2007-5791: September 2007). Internet. Found at http://idart.sandia.gov/methodology/materials/Adversary_Modeling/SAND2007-5791.pdf

9 Schneier, Bruce. *Modeling Security Threats - Attack Trees* (Reprint Dr Dobb's Journal: 1999. Counterpane Internet Security: 1999). Internet. Found at http://www.**schneier**.com/paper-attacktrees-ddj-ft.html

10 Penn State University SIIS Laboratory. *Advanced Metering Infrastructure Security.* **(**Penn State University Systems and Internet Infrastructure Security Laboratory, Computer Science and Engineering (CSE) Network and Security Research Center (NSRC): 2010). Internet. Found at http://siis.cse.psu.edu/smartgrid.html

11 *Ibid.* Penn State University, 2010

12 Atkins, William. *Read Teaming – It's Good to be Bad. (*Missouri S&T ACM SIG in Security. SANDIA Critical Infrastructure Systems Department, NM, 10 FEB 2010). Internet. Found at. *http://acm.device.mst.edu/security-files/2010-02-10-Red_Teaming.ppt*

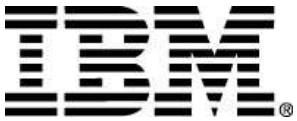
‡ See the supplemental paper that accompanies this presetation *titled* : Yanalitis, Mark. *RED TEAMING APPROACH, RATIONALE, AND ENGAGEMENT RISKS* (self-published: 2011). Internet. Found at http://www.mediafire.com

Integrating a Vendor Assessment Program Into Your Organization

Thomas H. Garrubba
Manager - Technical Assessments Group; CVS Caremark

Mission and Founding Members

Created by industry leaders to provide a standardized, risk-based approach to assess service provider control environments in a rational, cost-effective manner



Why Shared Assessments?

- Common sense answer to complex process
- Reduces costs
- Increases efficiencies
- Global acceptance
- One-stop shop for meeting federal regulations and international standards

SHARED ASSESSMENTS

CVS CAREMARK

Why Shared Assessments?

- Raises the bar on risk management and controls
- Member-driven, member-funded
- Used by
  - financial services
  - healthcare
  - telecommunications
  - retail
  - higher education
  - energy
  - others
- Evolves to ensure relevance

SHARED ASSESSMENTS

CVS CAREMARK

Why Shared Assessments?

Efficiency

- **From 1000s of questionnaires to 1**
- Outsourcers get the information they need *immediately*
- Reduce or eliminate audit-related travel time

VW's 282 MPG Super Fuel Efficient Car

SHARED ASSESSMENTS

CVS CAREMARK

Why Shared Assessments?

- Service providers
  - Security message = competitive advantage
  - Evidence available during sales process
  - Can eliminate pre-sales audits
  - Can reduce the sales cycle

SHARED ASSESSMENTS

CVS CAREMARK

One-Stop Shop

ISO 27002 PCI-DSS HIPAA/HITECH

COBIT AICPA FFIEC

NIST GLBA UCF

SHARED ASSESSMENTS

CVS CAREMARK

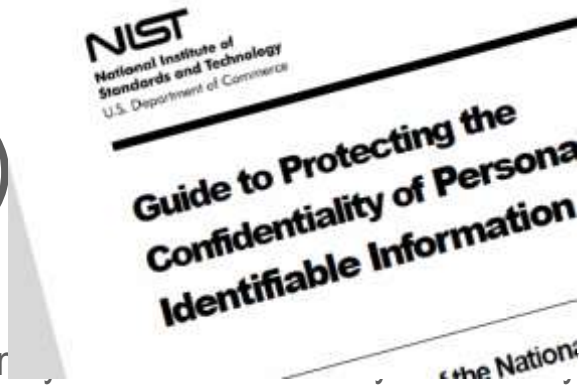
Case Study: CVS Caremark

Vendor Assessment Program – Implementation & Current Process

SHARED ASSESSMENTS

CVS CAREMARK

Confidential Data



Personally Identifiable Information (PII)

- Definition:
  - Includes any information that relates to an individual, whose iden… PII inferred, including any information that is linked or linkable to that individual regardless of the citizenship, age, or other status of the individual. This definition incorporates any patient medical records, protected health information, health care provider records, cardholder data, and employee employment data (including payroll and group health plan information).
- Examples:
  - Examples of personally identifiable information include employee badge numbers, Social Security Numbers, driver's license numbers, patient scripts, plan participant data, and credit card numbers.
  - Specifically, it incorporates any piece of information that can potentially be used to uniquely identify, contact, or locate an individual, such as name, address, date of birth, mother's maiden name, telephone number, participant ID number, Rx Number, or patient identifiers.
  - You will find PII on Caremark participant invoices or on a completed CVS/pharmacy ExtraCare Card application or in a MinuteClinic medical record.

SHARED ASSESSMENTS

Confidential Data

Cardholder Data (CHD) aka Payment Card Industry (PCI)

- Definition:
  - Credit or debit card information that includes the Primary Account Number (PAN), which is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Cardholder Data may also appear in the form of the full PAN and, and at least one of the following: (1) Cardholder name, (2) Expiration Date, or (3) Service Code (Three- or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction). The Payment Card Industry Data Security Standard (PCI-DSS) obligations the Company to protect this information. Note that Cardholder Data is also a type of PII as personal information associated with a credit or debit card.
- Examples:
  - Payment Card Receipt
  - Electronic Payment Card Transaction Record

Confidential Data

Protected Health Information (PHI, ePHI)

- Definition:
  - Any individually identifiable health information transmitted or maintained in any medium, including demographic information that is
    1. created or received by a health care provider, health plan or health care clearinghouse and (
    2. relates to past, present or future physical or mental health or condition of an individual, provision of health care to the individual, or payment for the provision of care to the individual, and
    3. identifies the individual or includes enough information about the individual so that there is a reasonable basis to believe that the information can be used to identify the individual.
  - PHI is a subset of PII because PHI is also linked to an individual, PII is considered PHI when linked with health information and is obtained by or on behalf of a health plan or health care provider. For example, when a patient's name appears on a prescription.

One or more PII data elements *Examples:*	Plus one or more health care data elements *Examples:*
Name	Disease state
Address	Prescription History
Date of Birth	Medical treatment or diagnosis
SSN	Health insurance Identification or account number

SHARED ASSESSMENTS

Confidential Data

Medicare Part D Data

- Description:
  - Federal regulations require that any vendor who performs any activities outside of the United States in support of Medicare Part D take extraordinary measures to ensure that offshore arrangements protect patient privacy. This requirement extends to any subcontractors used by vendors contracted with CVS Caremark.

SHARED ASSESSMENTS

Confidential Data

Sensitive Operational or Financial Information

- Description
  - Business Owner will consult with assigned Business Analyst if necessary to determine if the relationship is deemed of financial/operational significance.
- Examples:
  - Competitive Pricing
  - Advertising or Networking
  - Financial Information
  - Pricing Data
  - SEC Filing Data
  - Intellectual Property

SHARED ASSESSMENTS

Who Do We Assess?

- Any vendor that performs the following to our data:
  - Collect
  - Destroy
  - Store
  - Transmit/Transport
  - Process
- Remember: ***C-D-S-T-P!***

SHARED ASSESSMENTS

CVS CAREMARK

Why Do We Assess?

- To *mitigate* our exposure to a vendor's risk to our data (**note**: we do not *eliminate*!)
  - CVS Caremark – ***Due Diligence*** function
- We create *value* to the Business Unit and the Company
  - We provide "peace of mind" to the BU and the Company
    - **We look at items that BU's normally don't ask for (e.g.., SAS-70's, P/P's; Third Party SAS', P/P's; NVA/Pen-Tests, etc.)**
  - We provide "consultancy" services to vendors to ensure they hit generally accepted IT Standards

SHARED ASSESSMENTS

CVS CAREMARK

What are We to Assess?

- At what *level* do we look at the vendor?
  - Enterprise?
  - Geographic?
  - Business Line
  - Scope/Solution specific?
  - Combination of one or more of the above?

SHARED ASSESSMENTS

CVS CAREMARK

Formula for a Successful Program

- **P = p1(p2 + p3)** ***(Mortensen-Garrubba Theorem)***
  - **P** = Program
  - **p1** = Policy
  - **p2** = Process
  - **p3** = Practices

SHARED ASSESSMENTS

CVS CAREMARK

Formula for a Successful Program

- **P = p1(p2 + p3)**
  - **Policy** (*can* also be an Executive [CxO] Decree promulgated to the Organization)
    - "THOU SHALT…" statement;
    - ***Must Have*** in First Position!

SHARED ASSESSMENTS

CVS CAREMARK

Formula for a Successful Program

- **P = p1(p2 + p3)**
  - **Process** (series of *documented* actions or operations; Streamlined!)
    - May include items as:
      - SIG/AUP development and Usage
      - Internal & external resources
      - Documentation to review
      - Turnaround times;
      - How you communicate with the BU, vendor, your management
      - How you report to other Senior management levels (a "VAC")
      - "Contingent Items"; "Denials", etc.;

SHARED ASSESSMENTS

CVS CAREMARK

Formula for a Successful Program

- **P = p1(p2 + p3)**
  - **Practices** (your way of "doing things")
    - Making adjustments as needed (notifications; contingent items, etc.)
    - Does not *necessarily* need to be documented but must be *consistent* and *understood* by your management.

SHARED ASSESSMENTS

CVS CAREMARK

Defining Vendor Risks

- What is your data *at* risk?
  - PII?
  - PHI?
  - PCI?
  - Strategic?

Defining Vendor Risk

- What is your *data risk*? Ask yourself…
  - What is the *risk exposure (or "ranking")* to that data?
  - What is our *tolerance* of risk?
  - Is it calculated the same across the board (i.e., same for PII, PHI, PCI, Strategic, etc.)?

SHARED ASSESSMENTS

CVS CAREMARK

VAP Phase 1: Pre-Assessment

- Obtain all information you can regarding the scope of work for that vendor (read the SOW or contract!)
- Find out the data that will be CDSTP'ed
- Converse with the assigned BU and/or the vendor contacts to fully understand (**note**: *this can be your kickoff meeting!):*
  - ❑ *What* the vendor is doing
  - ❑ *Where* they will be doing it
  - ❑ *How* they will be doing it
- If applicable, determine if the assessment will be handled by an internal or external assessor
- Send the vendor the ***SIG*** questionnaire to be completed
- Determine if the assessor will perform Agreed Upon Procedures

SHARED ASSESSMENTS

CVS CAREMARK

VAP Phase 2: Assessment

- If you haven't had a kickoff meeting yet, now is the time!
  - Contacts?
  - Deliverables?
  - Timelines?
- Request/Review pertinent documentation:
  - BU Docs
    - Contracts, SOW's, NDA's, BAA's,
  - Vendor Docs
    - SAS-70/SSAE-16 /SOC-2 documents; ISO 27001/2 certifications, CMM Level, NAID, URAC, etc.
- Review the returned SIG Questionnaire responses

SHARED ASSESSMENTS

CVS CAREMARK

VAP Phase 2: Assessment

- Perform AUP
- Follow up on any questions regarding SIG responses
- Inform BU and vendor of any “contingent items” (i.e., audit issues/findings)
- Have a closing meeting to ensure CI’s are accurate
- Compose the Assessment Report
- Send Assessment Report to appropriate management (determined by *your* organization)
- File all work papers

SHARED ASSESSMENTS

CVS CAREMARK

VAP Phase 3: Post-Assessment

- Ensure you have a process to track contingent items
- Keep VAP management, BU management, and the vendor's management abreast of the progress or lack there of
- Get Sr. Level VAP and BU management involved if the vendor is:
  - Not communicating with you
  - Refuses to share data with you
  - Consistently misses remediation dates
- Review CI remediation documentation and if acceptable, close out the item

SHARED ASSESSMENTS

CVS CAREMARK

Contingent Items

- Contingent Items = “audit issues/findings”
  - Require remediation by the vendor or Business Unit
    - If the vendor/BU does not address them in the timely fashion prescribed, the vendor relationship may become in jeopardy!
  - Should be risk-rated and prioritized as such
  - Should be actively monitored by the VAP group responsible for closing these items
  - Should be escalated to appropriate levels of management if the remediation timelines are not met
  - Adjust the timelines if the vendor cannot *reasonably* meet the target dates (you need to decide if these timelines should be “set in stone”!)

SHARED ASSESSMENTS

CVS CAREMARK

Contingent Items – 3 Types of CI's

- **Contractual**
  - Contracts, SOW's, NDA's, BAA's
  - Incomplete
  - Out of date
- **HR-Related**
  - Drug testing
  - Background checks
  - Credit checks
- **Technical/Operations**
  - Typical IT/Operations-related issues/findings/observations

VAP Phase 3: Post-Assessment

- **Start planning for Reassessment!**
  - Maybe based on type of data (PCI, PHI, etc.)?
  - Maybe based on the geographic location?
  - Maybe based on a SIG scoring system?
  - Maybe based on an aggregate score card?

SHARED ASSESSMENTS

CVS CAREMARK

Other Items - External Assessors

- These are an *extension* of your VAP team and should be treated as such
  - Monitor their progress
  - Meet with them at least weekly
  - Ensure they pull you in when the assessment begins to "look bad" (no surprises!)
- Make sure other vendors will accept their NDA's
  - Be prepared for the Legal dept's to ~~red-line~~ much of the document!
  - Be prepared to adjust start/end dates
  - Insist *you* participate in the closing meetings for key/offshore vendors

SHARED ASSESSMENTS

CVS CAREMARK

Summary: Big "To Do's"

- Have executive buy-in (Remember: **P1**! MUST HAVE!)
- Establish a risk-based approach for prioritizing your assessments
- Establish core relationships with BUs (streamlines vendor communication); this leads to providing value to the BU
- Have the business unit (BU) establish initial contact with the vendor (i.e., they write the checks!) and be upfront as to what could happen if the vendor doesn't meet your organization's standards or Best Practices
- Use qualified assessors (CISAs, CISSPs, CRISCs. etc.)

SHARED ASSESSMENTS

CVS CAREMARK

Summary: Big "To Do's"

- Establish a follow-up process for contingent items
- Use the SIG and AUP's as your primary tools for assessing vendors
- Follow up on "Yes" and "No" answers in the SIG
- Share *contingent items* ("observations," "issues," "findings") with the BU and the vendor
- When feasible, use established professional assessment firms to assess your key high-risk vendors

SHARED ASSESSMENTS

CVS CAREMARK

Summary: Big "Do Not's"

- Treat your VAP as an administrative function
- Leave your VAP process ad hoc (remember: **(p2+p3)**)
  - Formalize it
  - Document it
- Keep BUs in the dark during the assessment process
- Wait too long to publish your assessment to the appropriate personnel
  - It's a point in time
- Treat any vendor assessment as a one-time deal
  - Schedule a risk-based reassessment

SHARED ASSESSMENTS

CVS CAREMARK

Questions/Answers

For More Information…

- www.sharedassessments.org
  - Resources
    - FAQs and tips for getting started
    - Case studies
    - Enterprise Cloud Computing Guide
    - Detailed comparisons with regulations and international standards (HIPAA/HITECH, PCI, ISO, COBIT, NIST)
  - Members
    - Membership: *Joyce Crawshaw, Client Relations Manager ; 505-466-6434; joyce@santa-fe-group.com*
    - Shared Assessments Tools: *Brad Keller, Senior Consultant; 980-875-9033; brad@santa-fe-group.com*
  - Partners
- Email thomas.garrubba@caremark.com or call 412-967-8196

Join us on LinkedIn!

SHARED ASSESSMENTS

CVS CAREMARK

Four Essential Requirements for Securing Your Enterprise

David C. Brown, CISSP, PMP, CEH

IUP Information Assurance Day 2011
November 10, 2011

Agenda

- Speaker
- Real Security Requires Focus
- How to REALLY Secure Your Enterprise
  - CEO View: Value, Growth, Protection
  - Shared Enterprise Reference Model
  - Discovering the As-Is State
  - Prioritizing: Using Business Goals as Guide
- Tie it All Together for Security
- Additional Benefits
- Action Summary

Speaker

- 30+ years experience in information technology and manufacturing business processes
- 20+ years experience addressing CyberSecurity
- Six Sigma Green Belt
- ITIL V3 Foundation for Service Management
- HIPAA, Security Analyst, Computer Forensics, etc…
- **MOST IMPORTANT:**

  Experience as a victim à la Morris Worm, 1988

Real Security Requires Focus

- **Business Goals**
- **7 Business Components**
- **Business Information Touch Points**

How to REALLY Secure Your Enterprise

1. CEO View: Value, Growth, Protection
2. Shared Enterprise Reference Model
3. Discovering the As-Is State
4. Prioritizing: Using Business Goals as Guide

David C. Brown, CISSP, PMP, CEH
www.BusinessCyberSecurity.com

A Perception Problem

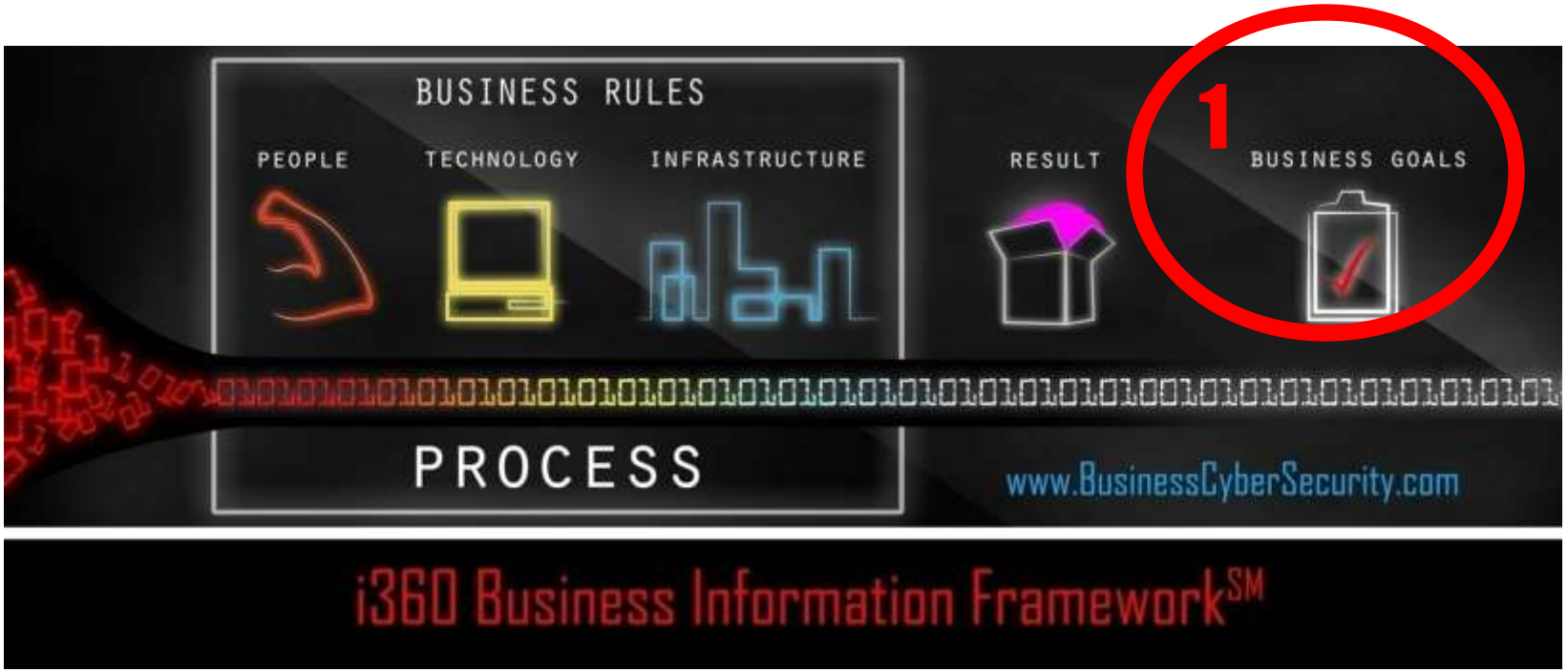
- Mark & Access Control
- My department, project, branch, etc is the most important
- What should be <u>everyone's viewpoint</u>?

1. CEO View: Value, Growth, Protection

How Do You Share CEO's View?

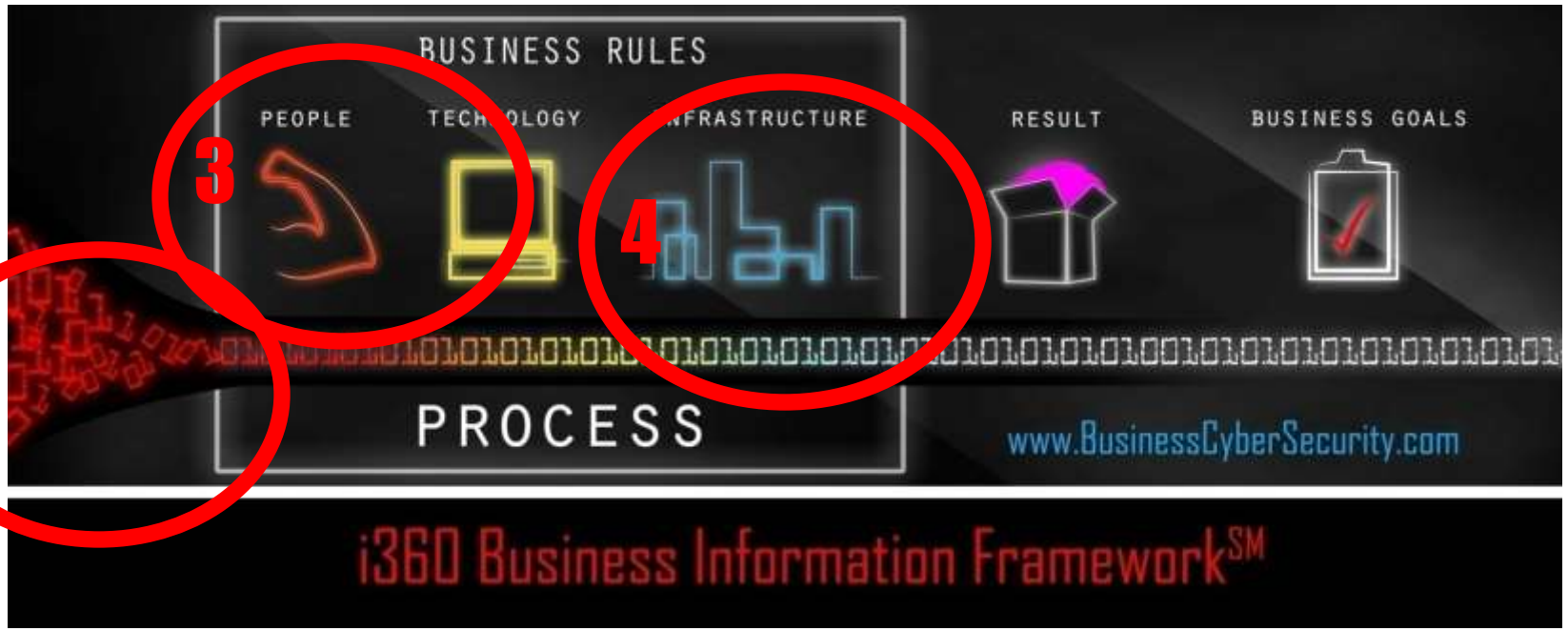
- Models:
  - Chair
  - Table
  - Business?

2. CEO's Reference Model



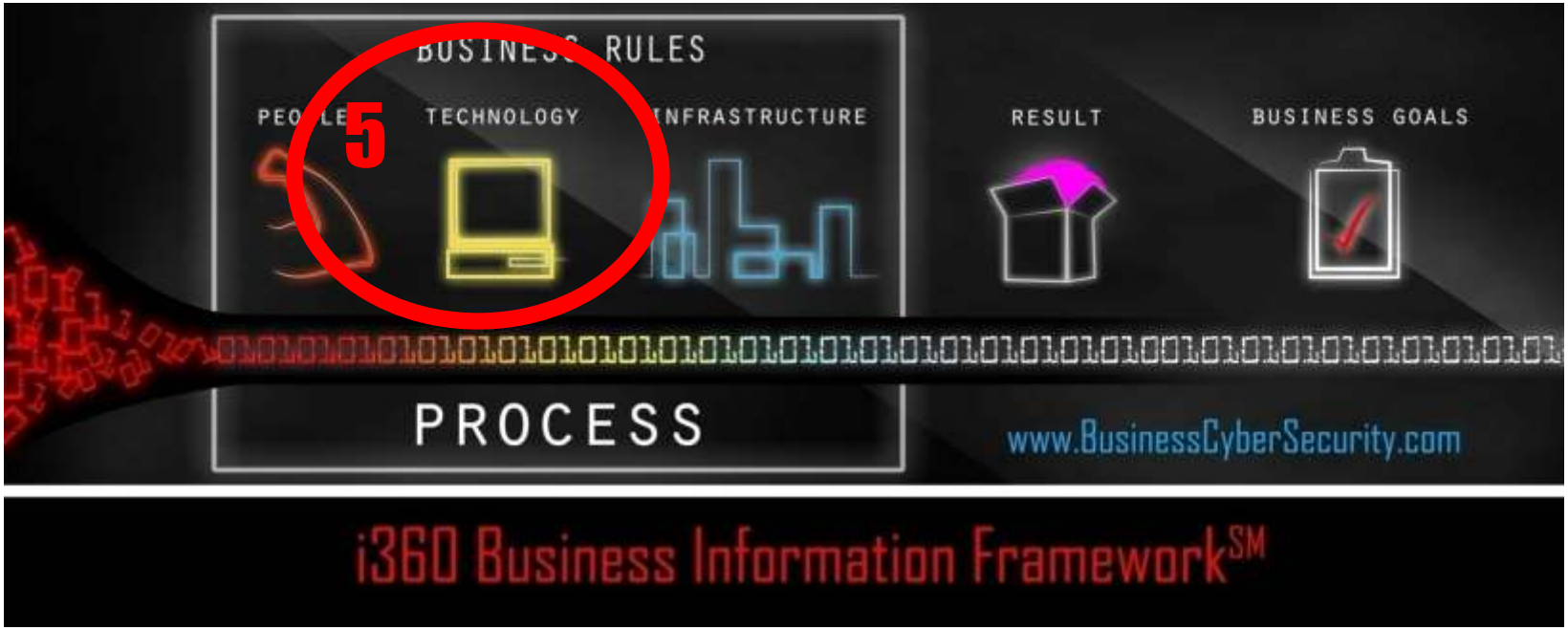
1. Business Goals – Value, Growth & Protection

CEO's Reference Model



2. Customer calls with an order. – Information
3. Employee takes order - People
4. Order transmitted over the network to a server - Infrastructure

CEO's Reference Model

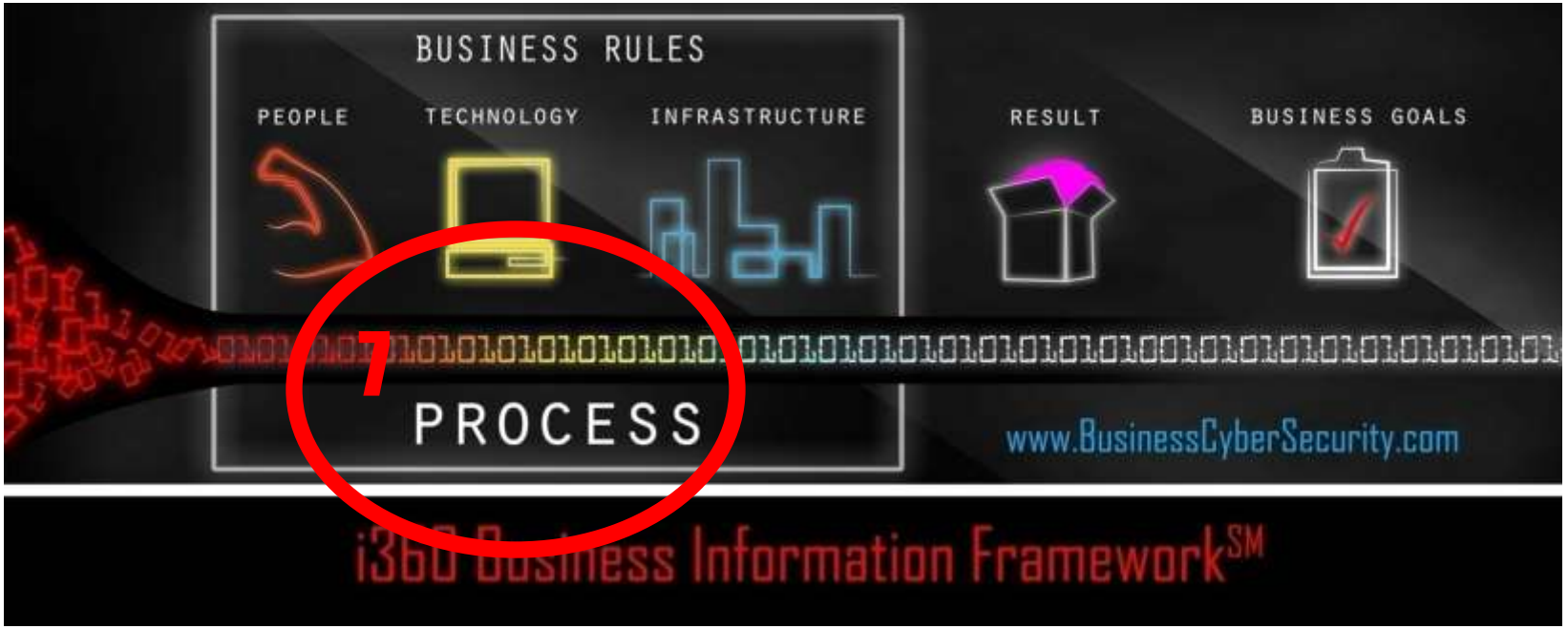


5. Given to application and entered into database - Technology

CEO's Reference Model

6. Credit limit, shipping restrictions check – Business Rules

CEO's Reference Model



7. Workflow management, sequencing – Business Process

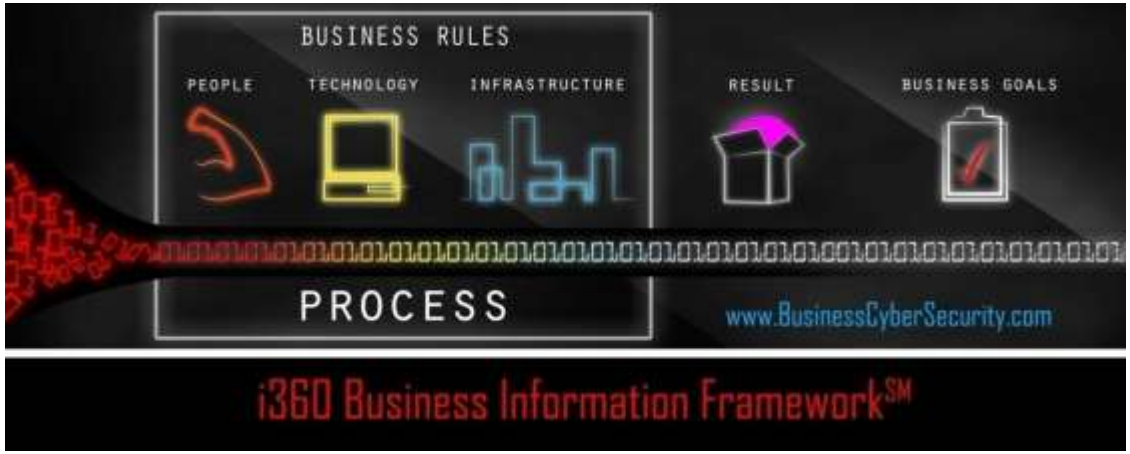
CEO's Reference Model

Many processes - All should be focused on Business Goals

- Patient intake/discharge/management
- Student enrollment/graduation
- Order processing
- Manufacturing
- Bank account creation
- Employee management
- Many more…

Value of Enterprise Reference Model

- Adds common structure to security assessment, risk assessment, BIA, BA, and audit tools
- Adds common structure to Six Sigma, ITIL, PCI, SOX, Audits, etc…
- Works for:
  - **any industry**
  - **any process**
  - **any company**
  - All use the same 7 business components

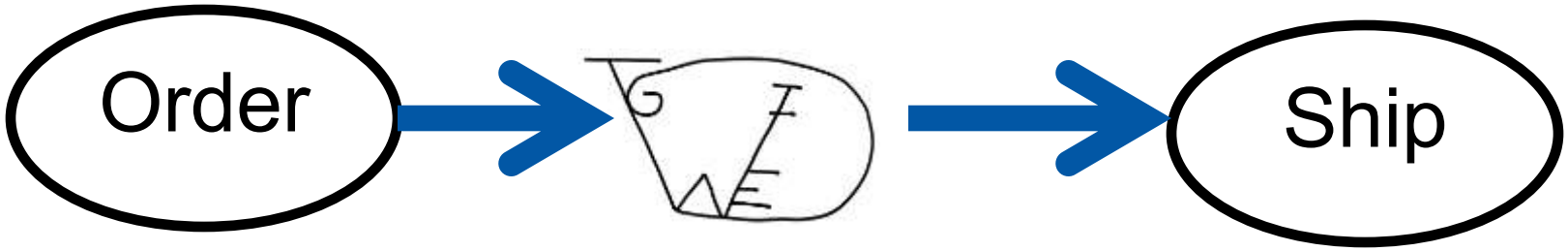


3. Quick Start: Where to Begin? Discovering the As-Is State

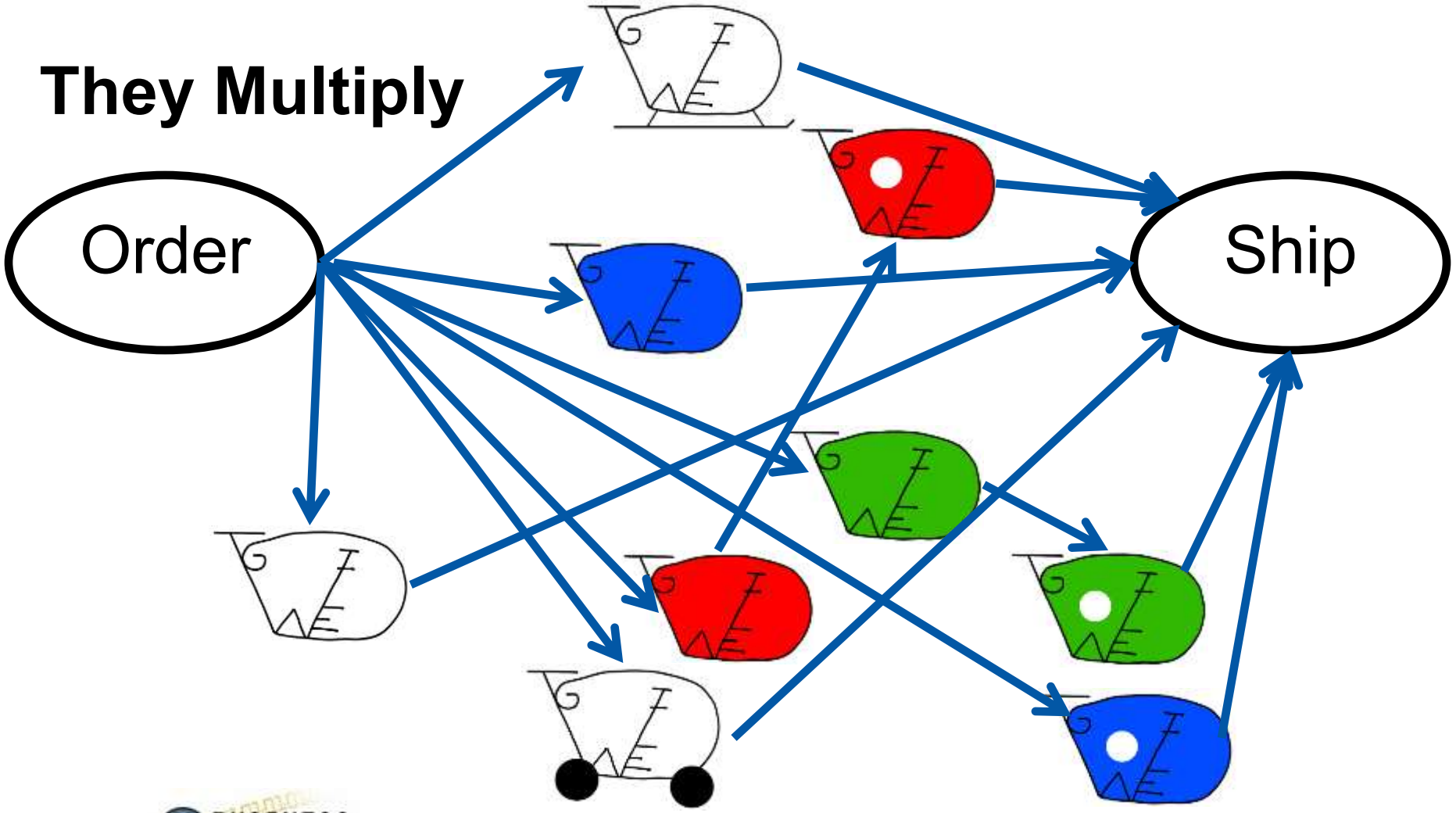
Business Process Mapping

- **Critical to understanding your enterprise**
- **Critical to security**
- **Starting point**

About Processes



Discovering the As-Is State



Automated Business Process Discovery (ABPD) Software

- Everything moving
- Nothing is removed – might break it & no time to fix
- Manual process mapping takes months, political, infrequent exceptions forgotten, ties up the everyone's time – Major effort
- ABPD software quickly maps business processes & discovers the business component relationships
- **<u>Weeks</u> not months – Enables Quick Start**

Prioritizing Among Equals

- ✓ CEO's perspective
- ✓ Shared perspective with all stakeholders
- ✓ Found & documented all processes

How do you balance all of the requirements?

Example:

•100' wall vs. Safety Deposit box

•Cloud vs. private cloud

4. Prioritizing: Keeping Business Goals as Guide

Component / Aspects	Biz Goals	Process	Biz Rules	People /Agent	Tech	Infra-Struct	Info
Confidentiality							
Integrity							
Availability							
ISO 900x Compliance							
Budget Requirements							
SOX-Compliance							
PCI-Compliance							
HIPAA-Compliance							
KPI Metrics							
etc...							

Prioritizing: Keeping Business Goals as Guide

Example analysis

Business Goals

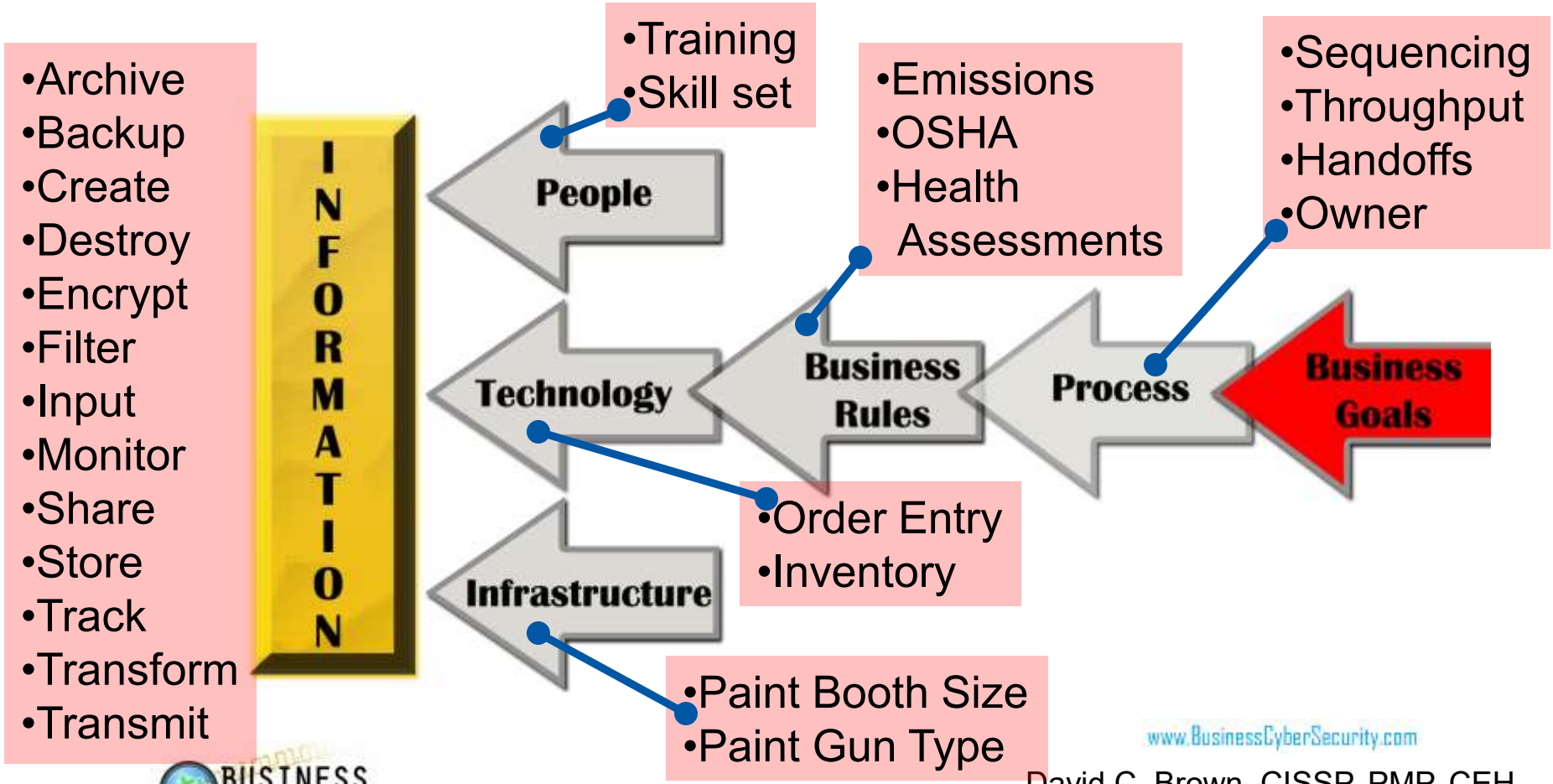
Confidentiality

- **Competition**
- **Partners**
- **Budget**
- **Etc…**

www.BusinessCyberSecurity.com

Short Walkthrough

Example – Reduce cost of blue widgets



TruBPI^{SM} Analysis Chart

- Not replacement for existing analysis tools
- Multiplies the power of existing security assessment, risk assessment, BIA, BA, & audit tools
- Guides prioritization of funding for business efforts
- Identifies gaps
- Helps determine business requirements
- Reveals true scope of required changes
  - It's not just one project

TruBPI^{SM} Analysis Chart

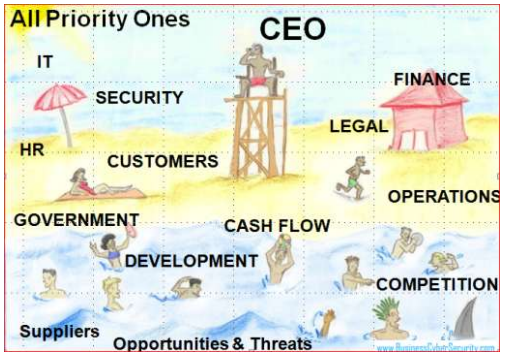
- Make the chart as detailed as you want
- Include SMEs from every part of the organization
- Don't expect to do it overnight
- Mine has taken quite a while to build

Here's some of the sources and areas that I used to build my TruBPI Analysis chart:

21 CFR PART 11 (FDA- Clinical)
45 CFR PART 160(HIPAA)
45 CFR PART 164(HIPAA)
Archiving best practices
Automatic Process Discovery Tools
Automation
BA (Business Analysis)
Balanced Scorecard
BAM (Business Activity Monitoring)
BCP (Business Continuity Planning)
BI Business Intelligence
BIA (Business Impact analysis)
BIM (Building Information Modeling and Management)
BRMS (Business Rule Management System)
BRMS (Business Rules management Sys)
BRP (Business Recovery Planning)
Business Analysis Book of Knowledge
Business Management Principles
Business Process Analysis
Business Process Discovery
Business process improvement
Business Process Management Systems (ActiveVOS, ARIS, Nimbus etc.…)
Business Process Mapping
Business Process Model Notation (BPMN)
Business Process Modeling
Business Requirements Analysis Tools
Business service management (BSM)
Business Strategy
Call Center Design and Management
CCNA (Cisco Certified Network Associate) certification study materials
CEH (Certified Ethical Hacker) certification study materials
Change request management principles
CHFI (Computer Hacking Forensic Investigator)
Civil Litigation Procedures
Cloud computing and security
CMMI (Capability Maturity Model Integration)
CobiT (Control Objectives for Information and Related Technology)
COCO (Criteria of Control)
Computer Forensics
Continuous improvement methods
COSO(Committee of Sponsoring Organizations of the Treadway Commission)
CRM (Customer Relationship Management) procedures and principles
Cryptography/Encryption
Database management
Deduplication
DLP (Data Loss Prevention)
Document Management system
DODAF (Department of Defense Architecture Framework)
DPA (Data Protection Act 1998 European)
DR (Disaster Recovery planning)
Early Case Assessment
ECM (Electronic Content Management Systems)
ECSA (EC council certified security analyst) Certification study materials
eDiscovery
EDRM (Electronic Discovery Reference Model)
Email Classification
Email Security
Embedded Security
Enterprise Architecture
ERP/COSO (Enterprise Risk Management)
eTOM (Enhanced Telecom Operations Map)
FEA (Federal Enterprise Architecture) Framework
Federal Rules of Evidence
FERPA (Family Educational Rights and Privacy Act)
FFIEC (Federal Financial
GAAP (Generally Accepted Accounting Principles)
GLBA (Gramm-Leach-Bliley Act of 1999)
Government Information Classification systems
GRC (Governance, Risk and Compliance)
Grid Computing
Hacker tools and methods
HIPAA (Health Insurance Portability and Accountability Act of 1996)
HIPAA and Healthcare information classification
HITECH (Health Information Technology for Economic and Clinical Health Act)
Host Security Management
Human Resource Management Principles
Identity Management
IFRS (International Financial Reporting Standard(s))
Incident Management
Incident Response
Information assurance
Information Classification
Information controls and management
Infrastructure management
ISO 27001 & ISO 27002
ITIL Service management, Lean Sigma
Log file management methods
MA 201 CMR 17
Managed Security Services
MCDBA (Microsoft Certified Data Base Administrator) certification study materials
MCSE (Microsoft Certified System Engineer) certification study materials
Mergers and Acquisition procedures
Military Classification systems
Mobile Device Management (MDM)
Mobile device management and Security
Navy Information assurance manual
Network based Intrusion
Patch management
PCI-DSS compliance requirements,
Penetration testing
Physical security methods and procedures
PMP (Project Management Professional) certification study materials
Policy management and creation
Process automation
Process Discovery
Process Governance Best Practices Healthcare PII, eHR Security Management Best Practices
REACH (Registration, Evaluation, Authorization and Restriction of Chemicals)
Records Classification
Records Information Management best practices
Remote access controls
Risk Assessment
Risk management
SaaS (software as a Service)
SCOR (Supply Chain Operations Reference model)
Secure Application development and programming practices
Secure Business Process Management
Security Awareness Training
Server Management Practices
SIEM (Security Incident Event Management Practices)
SIPOC (Suppliers Inputs, Process, Outputs, Customers)
Six Sigma certification study materials
SOA (Service Oriented Architecture)
Social Media security mgmnt
SOX (Sarbanes-Oxley Act of 2002)
State Laws (Numerous)
Supply Chain management and security
System Administration
TOGAF (The Open Group Architecture Framework)

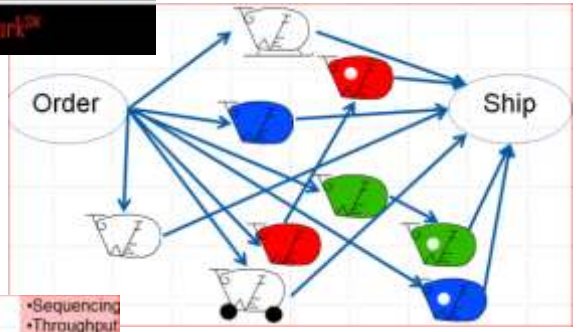
Tie It All Together for Security

1. **Focus**: On all information touch points, CEO View

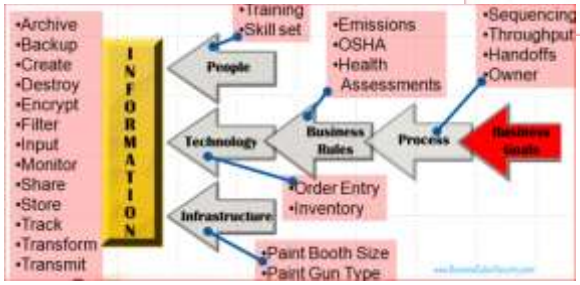


2. **Share**: i360 Business Information Model

3. **Quickly** capture "As-Is state": ABPD software tool



4. **Prioritize** time & resources



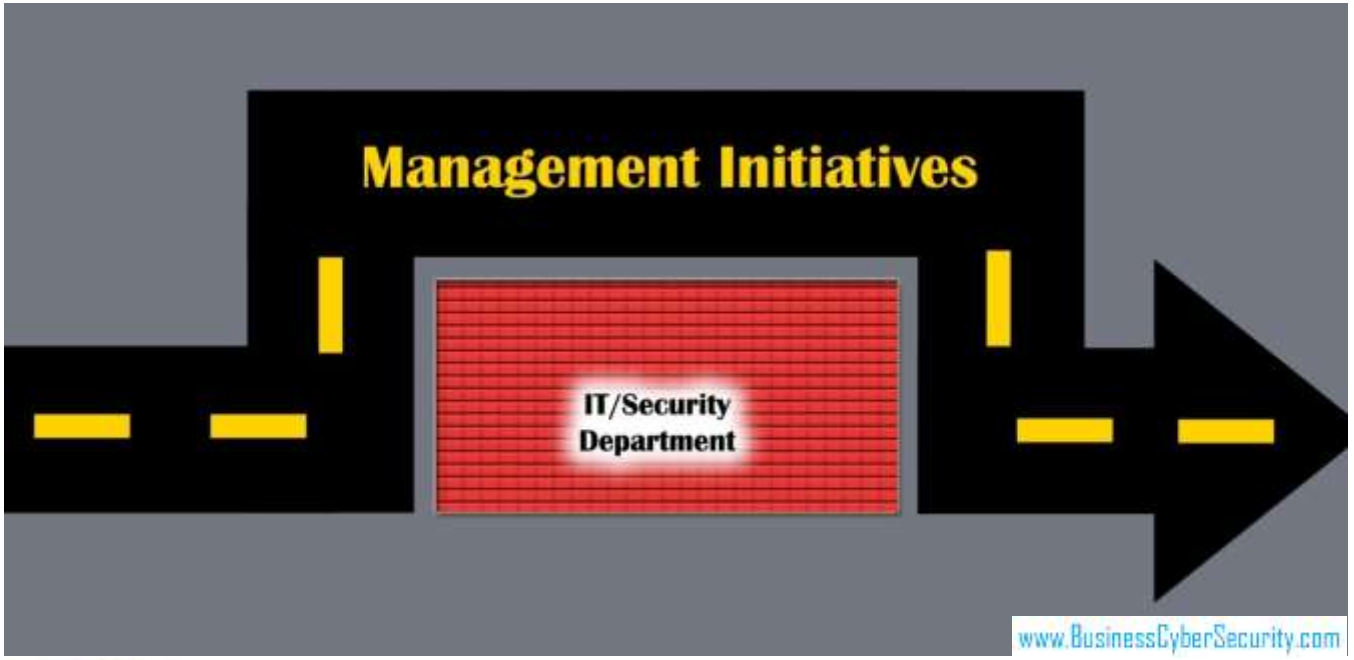
Additional Benefits

- Responsiveness - new opportunities
- Reduced cost/time for compliance audits
- Reduced cost/time litigation costs – eDiscovery
- Business Intelligence & Balanced Scorecard implementation readiness

- Extremely FOCUSED on Business Goals

Security & IT – Why You're NOT in the Loop

- Release Deadline vs. Process – Dave vs. Guard
- CEOs Hate “No” – You MUST add value
- You are still going to be held responsible



Action Summary for Security

1. **CEO must be directing – Not a handoff**
2. **Tell your CEO**
3. **Our thinking must change - CEO View**
4. **Not a quick fix – No Shortcut**
5. **Start small 1 process – Pilot project**
6. **Implement in 3 month steps – Short steps**
7. **Continuous improvement – Never stops**
8. **Learn more - signup for our newsletter**

David C. Brown, CISSP, PMP, CEH
www.BusinessCyberSecurity.com