SECURITY TESTING: THE MISSING LINK IN INFORMATION SECURITY

RANDALL W. RICE, CTAL (FULL), CTAL-SEC
RICE CONSULTING SERVICES, INC.
WWW.RICECONSULTING.COM

Most organizations do not know the true status of their information security because they have never actually tested it!

Many security vulnerabilities could be identified and eliminated - if a wider, more robust view of security testing were promoted and performed.

THE CHECKLIST

		Correctly applied and working effectively?
• Firewall installed?	☑	?
• Intrusion detection installed?	☑	?
• Encryption applied?	☑	?
• Internal controls in place?	☑	?
• Security policies and procedures defined?	☑	?
• Physical security in place?	☑	?
• Authentication and authorization applied?	☑	?

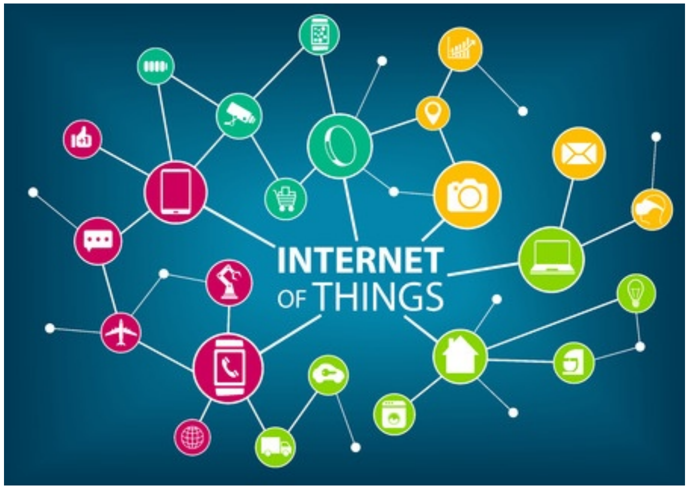
THINK ABOUT YOUR HOME SECURITY

- **Would you feel safe if…**
  - You only checked the doors were locked once a month?
  - You had an alarm system but never actually heard the alarm sound?
  - You had alarm monitoring but had never been called by the monitoring company when the alarm is tripped?
  - You had no personal protection plan?

Yet, This is How Many People Think About Security Testing.

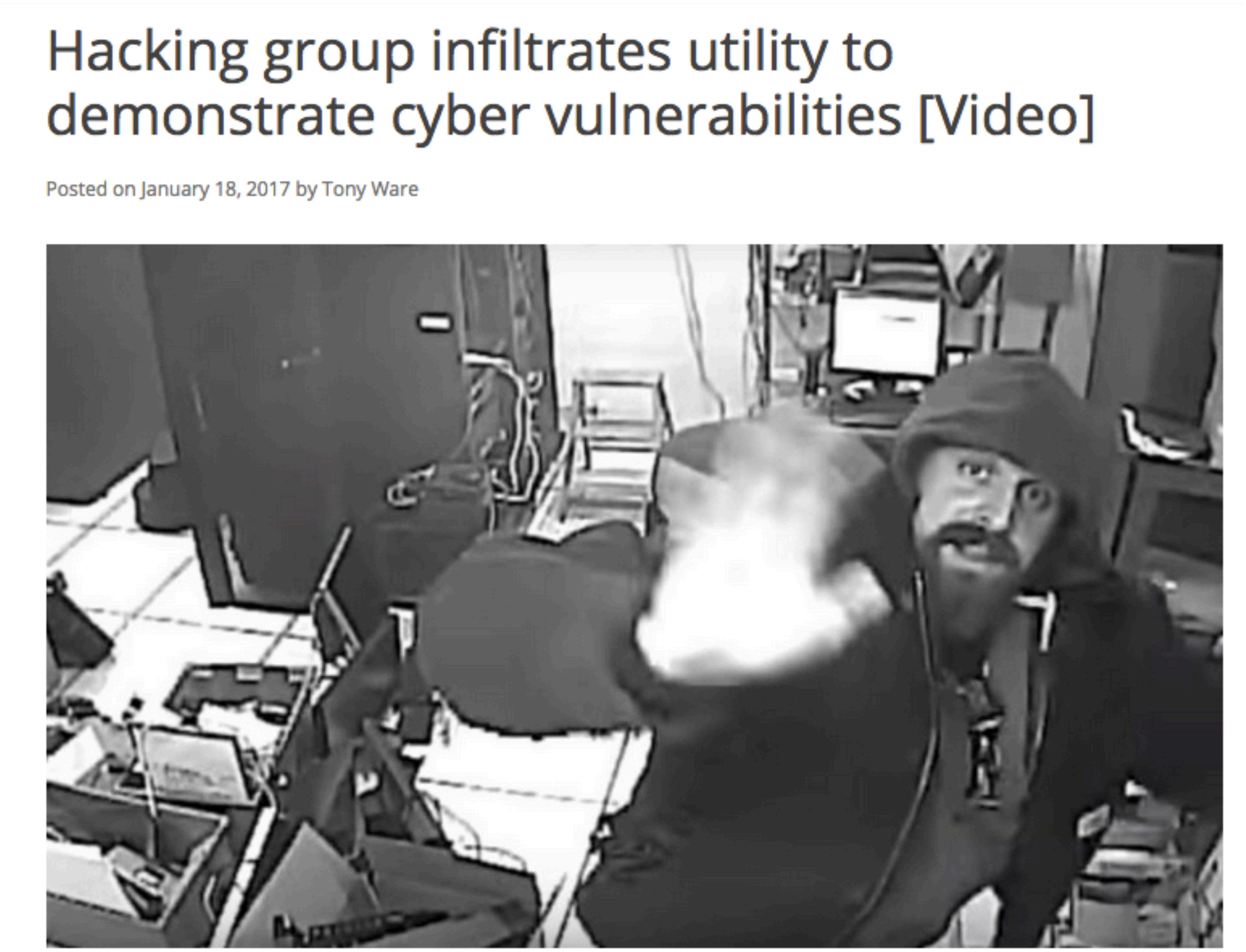
Security Testing is Not an Event.

It Should be a Continuous Activity.



SEE HOW A WHITE HAT HACKING GROUP BROKE INTO AN ELECTRICAL UTILITY COMPANY

- **Hacking group infiltrates utility to demonstrate cyber vulnerabilities [Video]**
  - http://fifthdomain.com/2017/01/18/hacking-group-infiltrates-utility-to-demonstrate-cyber-vulnerabilities/



Hacking group infiltrates utility to demonstrate cyber vulnerabilities [Video]

Posted on January 18, 2017 by Tony Ware

OBSERVATIONS

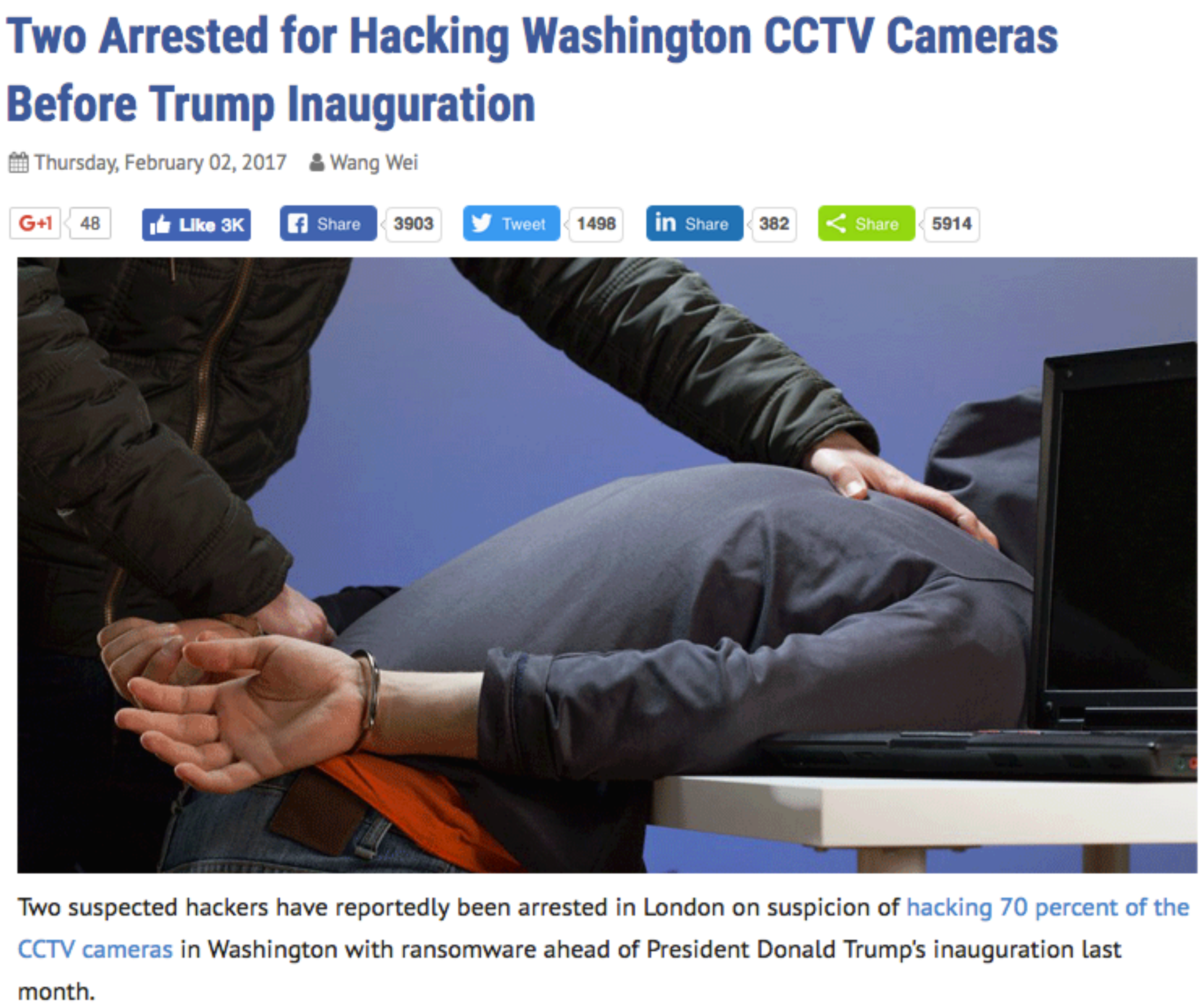
- **The target was a small rural co-op with incomplete security.**
    - A partial fence. Really?
- **The attacks were fairly low-tech at points.**
- **This is a great example of how exposed many small to mid-sized entities are, such as:**
    - Utilities
    - Healthcare (small Dr. offices, clinics, etc.)
    - Banks (community banks)
    - Airports (regional, general aviation)

DATA BREACHES CONTINUE TO CLIMB

- **Data Breaches Exposed 4.2 Billion Records In 2016**
  - The 4,149 data breaches reported in 2016 shattered the all-time high of nearly 1 billion exposed records in 2013.
  - http://www.darkreading.com/attacks-breaches/data-breaches-exposed-42-billion-records-in-2016/d/d-id/1327976

DATA BREACHES CONTINUE TO CLIMB (2)

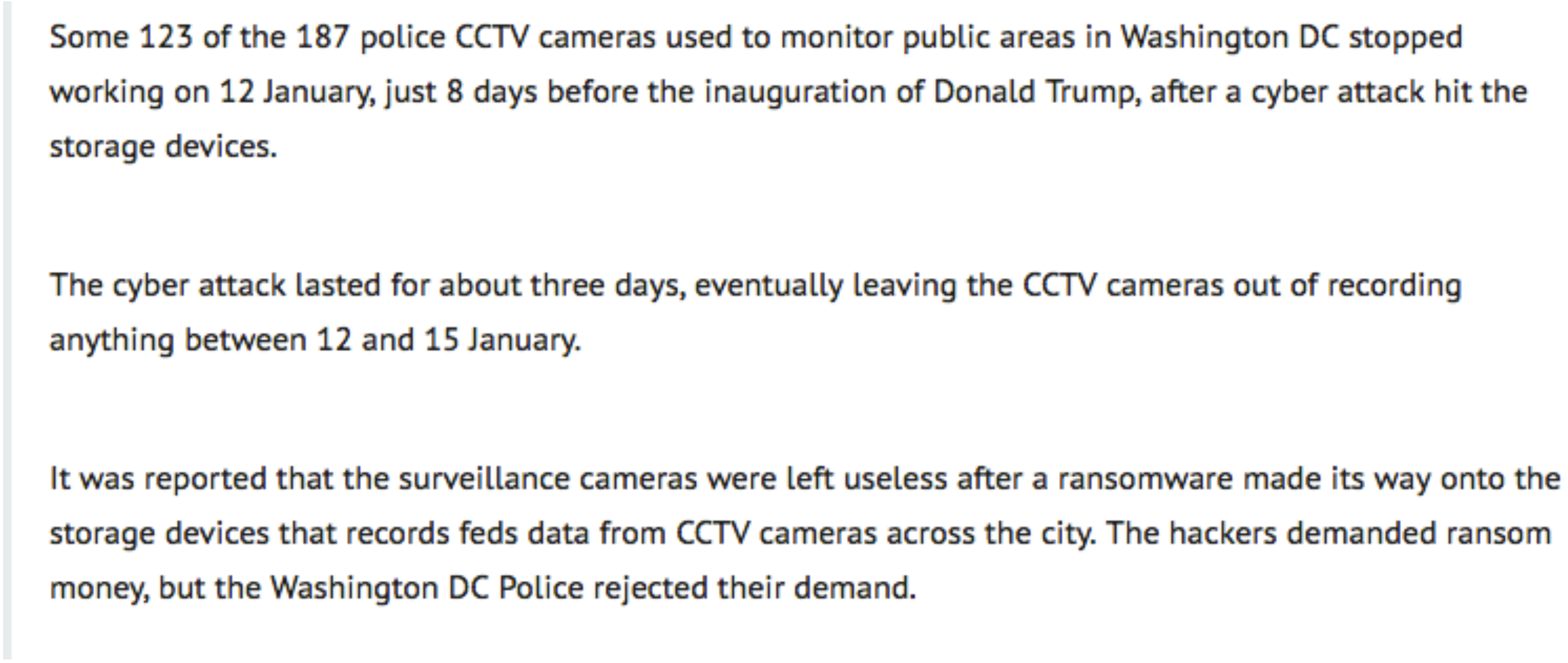
- In 2016, there were 94 reported incidents exposing at least one million records each, and 37 incidents exposing ten million or more records.
- Compared with 2015, this marks an increase of 63% and 105%, respectively.



Two Arrested for Hacking Washington CCTV Cameras Before Trump Inauguration

Thursday, February 02, 2017 Wang Wei

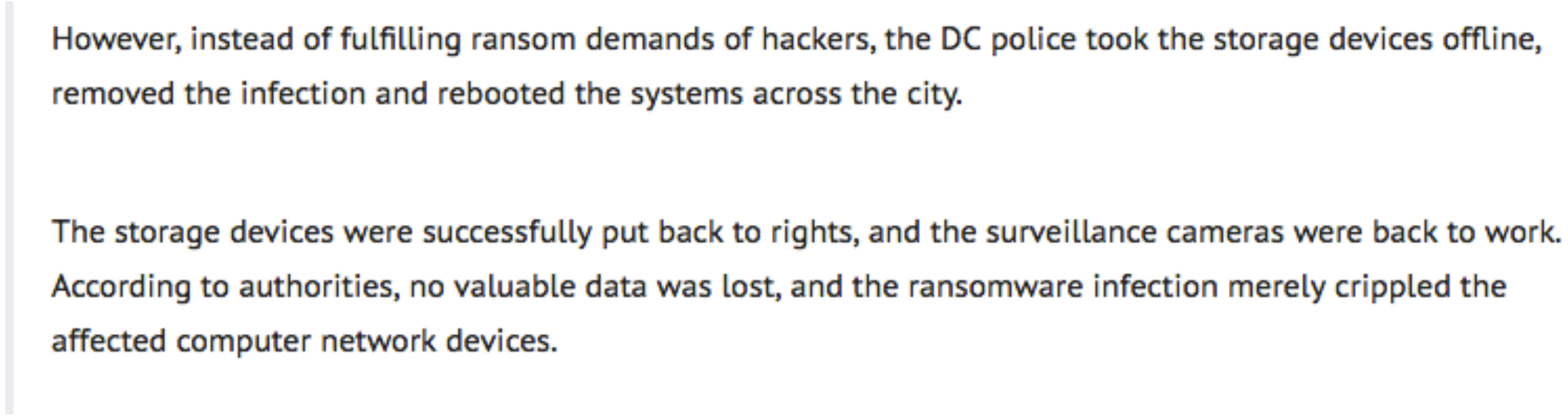
Two suspected hackers have reportedly been arrested in London on suspicion of hacking 70 percent of the CCTV cameras in Washington with ransomware ahead of President Donald Trump's inauguration last month.



Some 123 of the 187 police CCTV cameras used to monitor public areas in Washington DC stopped working on 12 January, just 8 days before the inauguration of Donald Trump, after a cyber attack hit the storage devices.

The cyber attack lasted for about three days, eventually leaving the CCTV cameras out of recording anything between 12 and 15 January.

It was reported that the surveillance cameras were left useless after a ransomware made its way onto the storage devices that records feds data from CCTV cameras across the city. The hackers demanded ransom money, but the Washington DC Police rejected their demand.



> However, instead of fulfilling ransom demands of hackers, the DC police took the storage devices offline, removed the infection and rebooted the systems across the city.
>
> The storage devices were successfully put back to rights, and the surveillance cameras were back to work. According to authorities, no valuable data was lost, and the ransomware infection merely crippled the affected computer network devices.

BIG CHALLENGES FOR THE U.S. FEDERAL GOVERNMENT

"…in fiscal year 2015, 19 of the 24 major federal agencies covered by the Chief Financial Officers Act of 1990 reported that **information security control deficiencies were either a material weakness or significant deficiency in internal controls over financial reporting.** In addition, **inspectors general at 22 of the 24 agencies cited information security as a major management challenge for their agency**."

Testimony Before the President's Commission on Enhancing National Cybersecurity – Sept. 19, 2016

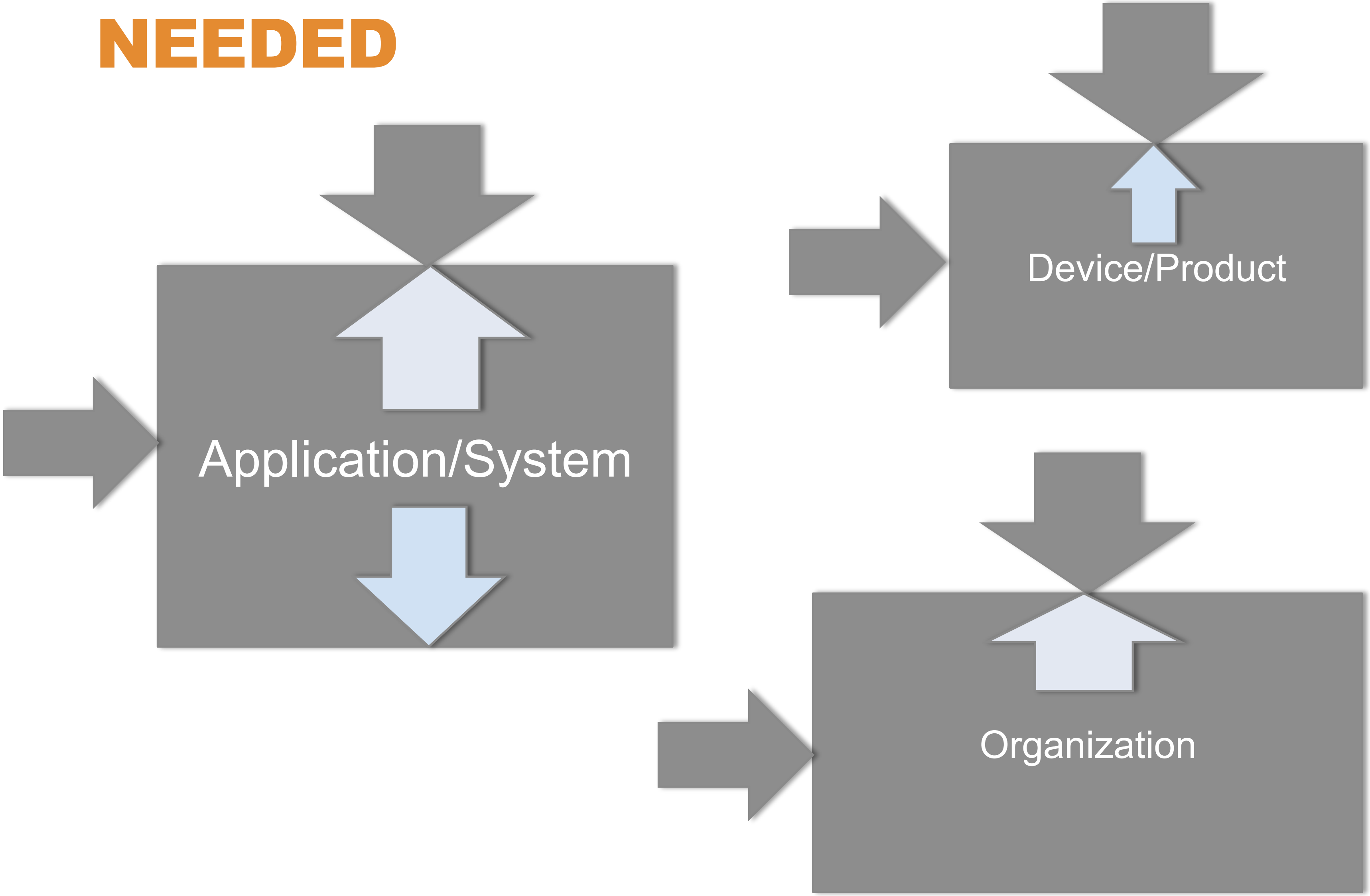
http://www.gao.gov/assets/680/679877.pdf

TO SEE HOW EASY THIS IS...

- **Google Hacking Database**
  - https://www.exploit-db.com/google-hacking-database/
- **Shodan**
  - https://www.shodan.io/

IMPORTANT: This is for illustrative purposes only. Unauthorized access of digital assets is a felony, even if the assets are unprotected.
https://www.law.cornell.edu/uscode/text/18/1030

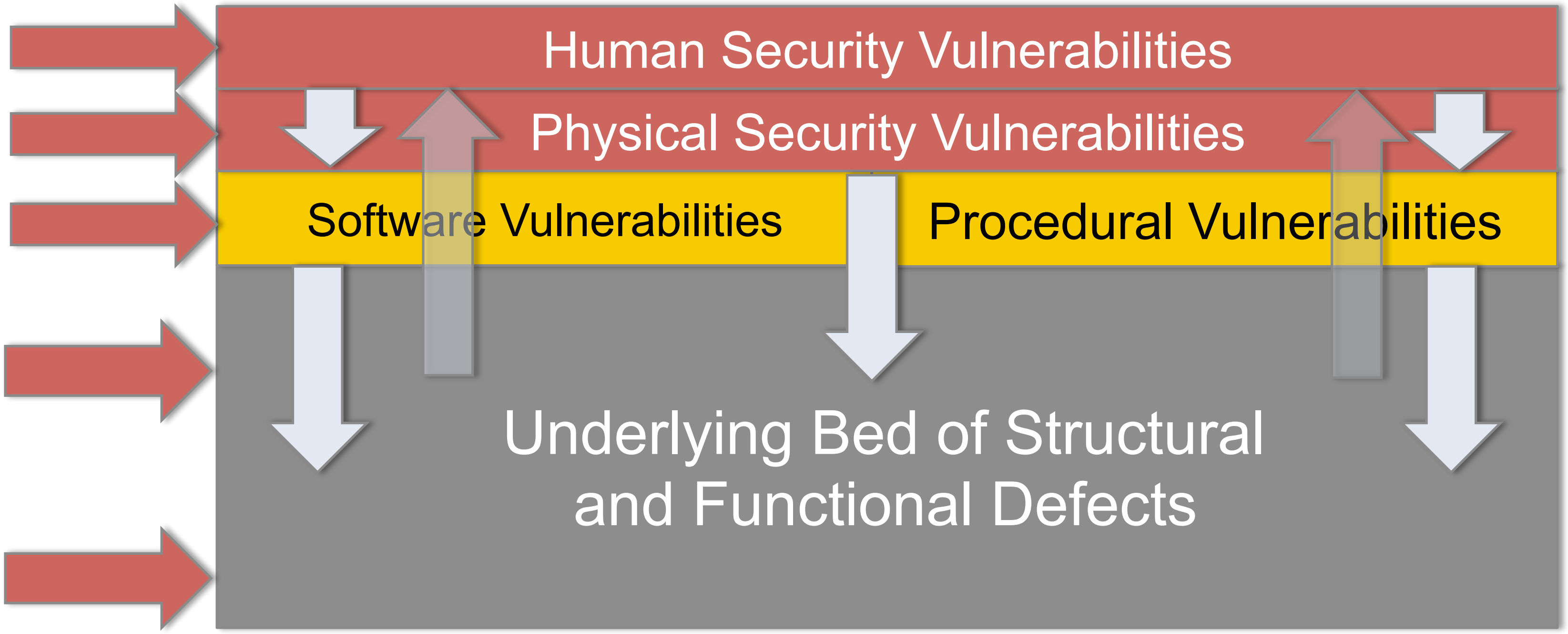
BOTH INTERNAL AND EXTERNAL VIEWS ARE NEEDED



WHY DO THE SECURITY BREACHES CONTINUE TO OCCUR?

- **Human lapses**
- **Malicious insiders**
- **Malicious outsiders**
- **Lack of adequate defenses and testing of the defenses that *are* in place**
- **Defective software in general**
- **A limited view of security and testing**
- **Placing too much trust in technology**
- **Security is an afterthought in most development projects**
- **Lack of awareness at the executive level**
  - Everybody knows cybersecurity is a problem, but very few people know how to deal with the risks and challenges.

THE NATURE OF DEFECTS


Human Security Vulnerabilities
Physical Security Vulnerabilities
Software Vulnerabilities
Procedural Vulnerabilities
Underlying Bed of Structural and Functional Defects

The impact of defects (of any type) can migrate throughout an organization.

WORK HOURS AND COSTS FOR DEFECT REPAIRS

	Defect Origins	Work Hours	Costs ($75 per hour)
1.	Security defects	10.00	$750.00
2.	Design defects	8.50	$637.50
3.	Requirements creep defects	8.00	$600.00
4.	Requirements defects	7.50	$562.50
5.	Structural defects	7.25	$543.75
6.	Architecture defects	7.00	$525.00
7.	Data defects	6.50	$487.50
8.	Bad fix defects	6.00	$450.00
9.	Web site defects	5.50	$412.50
10.	Invalid defects	4.75	$356.25
11.	Test case defects	4.00	$300.00
12.	Code defects	3.00	$225.00
13.	Document defects	1.75	$131.50
14.	Duplicate defects	1.00	$75.00
	AVERAGES	5.77	$432.69

Maximum can be > 10 times greater

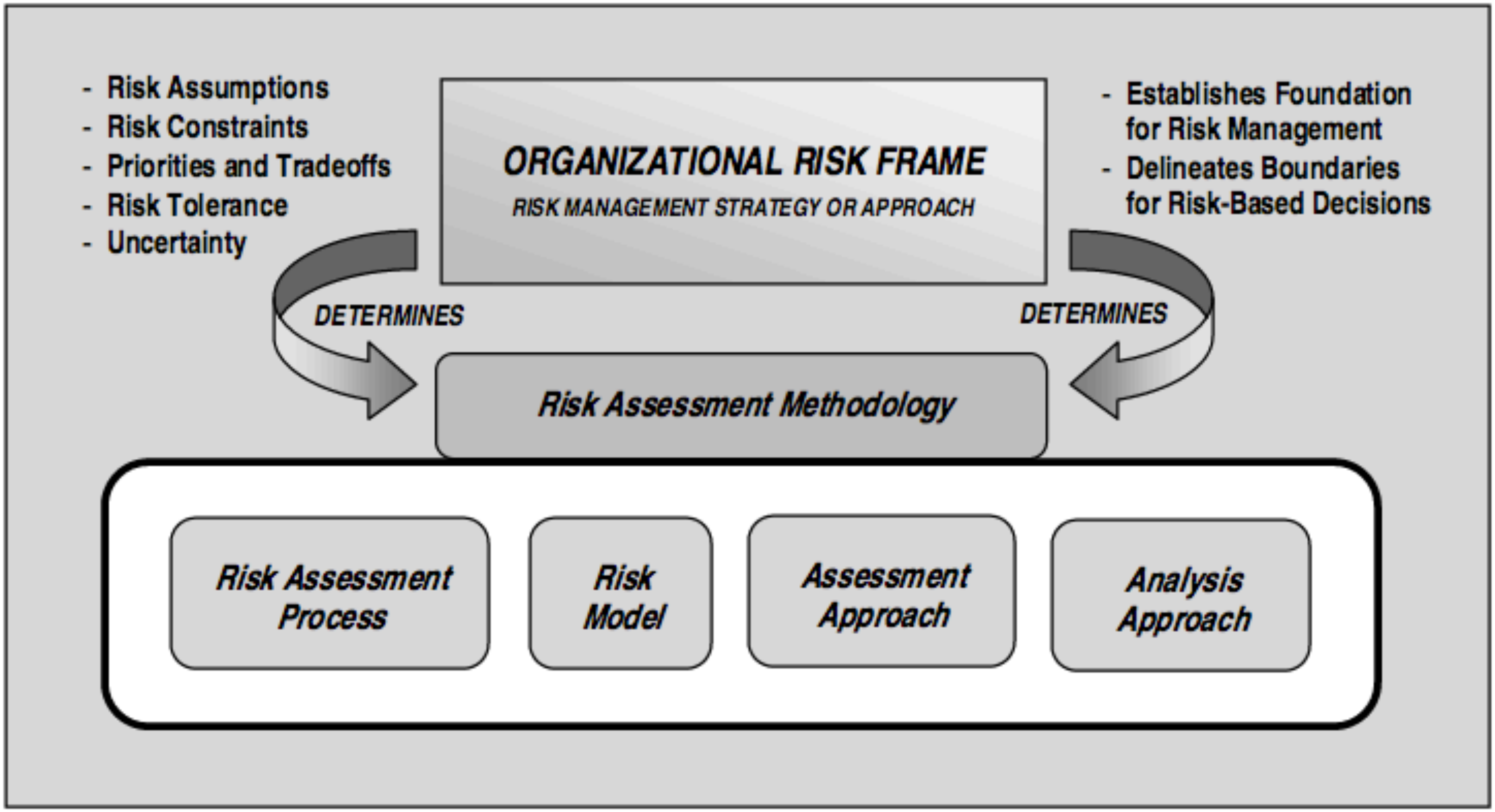
DEFECT DAMAGES AND RECOVERY COSTS

Defect Origins

1.	Security defects	$200,000,000
2.	Design defects	$175,000,000
3.	Requirements defects	$150,000,000
4.	Data defects	$125,000,000
5.	Code defects	$100,000,000
6.	Structural defects	$95,000,000
7.	Requirements creep defects	$90,000,000
8.	Web site defects	$80,000,000
9.	Architecture defects	$80,000,000
10.	Bad fix defects	$60,000,000
11.	Test case defects	$50,000,000
12.	Document Defects	$25,000,000
AVERAGES		$102,500,000

Defect recovery costs for major applications in large companies and government agencies

THE NIST RISK MODEL


- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

NIST Publication 800-30, Revision 1 – Guide for Conducting Risk Assessments (9/2012)

FOR FURTHER REFERENCE

- **NIST Publication 800-30, Revision 1 – Guide for Conducting Risk Assessments (9/2012)**
  - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

WHAT IS "HACKING"?

- **"The essence of hacking is finding unintended or overlooked uses for the laws and properties of a given situation and then applying them in new and inventive ways to solve a problem – whatever it may be be."**
  - Jon Erickson, *Hacking: The Art of Exploitation, 2nd Ed.*

THE ESSENCE OF HACKING

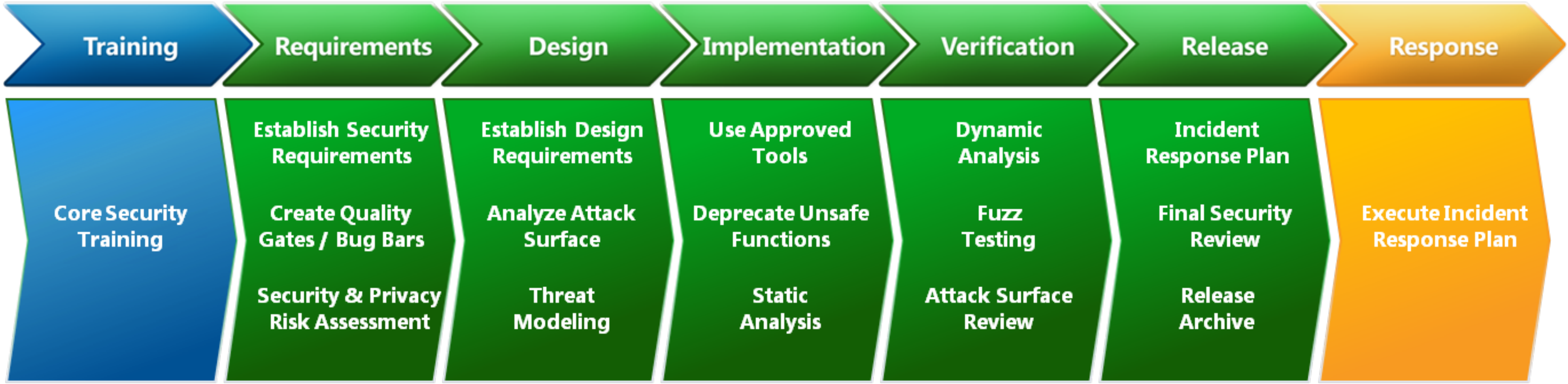
- Therefore, hacking may be performed for positive reasons, such as to show vulnerabilities,
- Or… hacking may be performed for malicious purposes.

GETTING THE ATTACKER PERSPECTIVE

- **To gain the attacker perspective, you must be able to think outside of norms and boundaries.**
  - In other works, be able to think like a hacker.
- **This is a big shift and challenge for many testers who are used to following test cases and test scripts.**
  - While testware can be helpful and confirmatory, in security testing, it often fails to discover vulnerabilities.

Three Examples of Security Lifecycle Models

MICROSOFT SECURITY DEVELOPMENT LIFECYCLE



Training	Requirements	Design	Implementation	Verification	Release	Response
Core Security Training	Establish Security Requirements Create Quality Gates / Bug Bars Security & Privacy Risk Assessment	Establish Design Requirements Analyze Attack Surface Threat Modeling	Use Approved Tools Deprecate Unsafe Functions Static Analysis	Dynamic Analysis Fuzz Testing Attack Surface Review	Incident Response Plan Final Security Review Release Archive	Execute Incident Response Plan

Reviews?

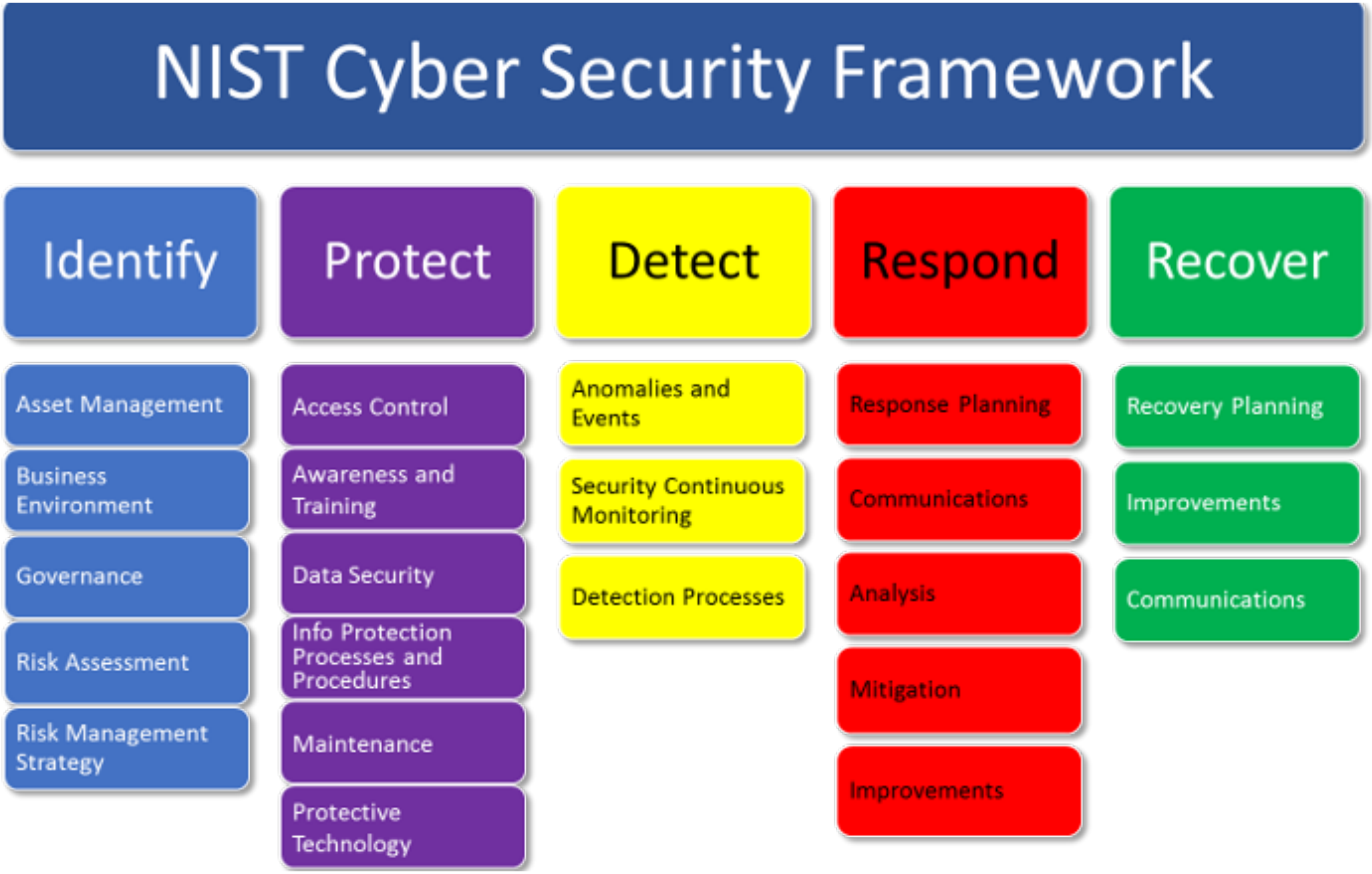
Reviews?

Secure Coding Methods?
Unit Tests for Security?

Functional Security Testing?
Structural Security Testing?
Pen Testing?

Incident Response Testing?
Security Configuration Testing?

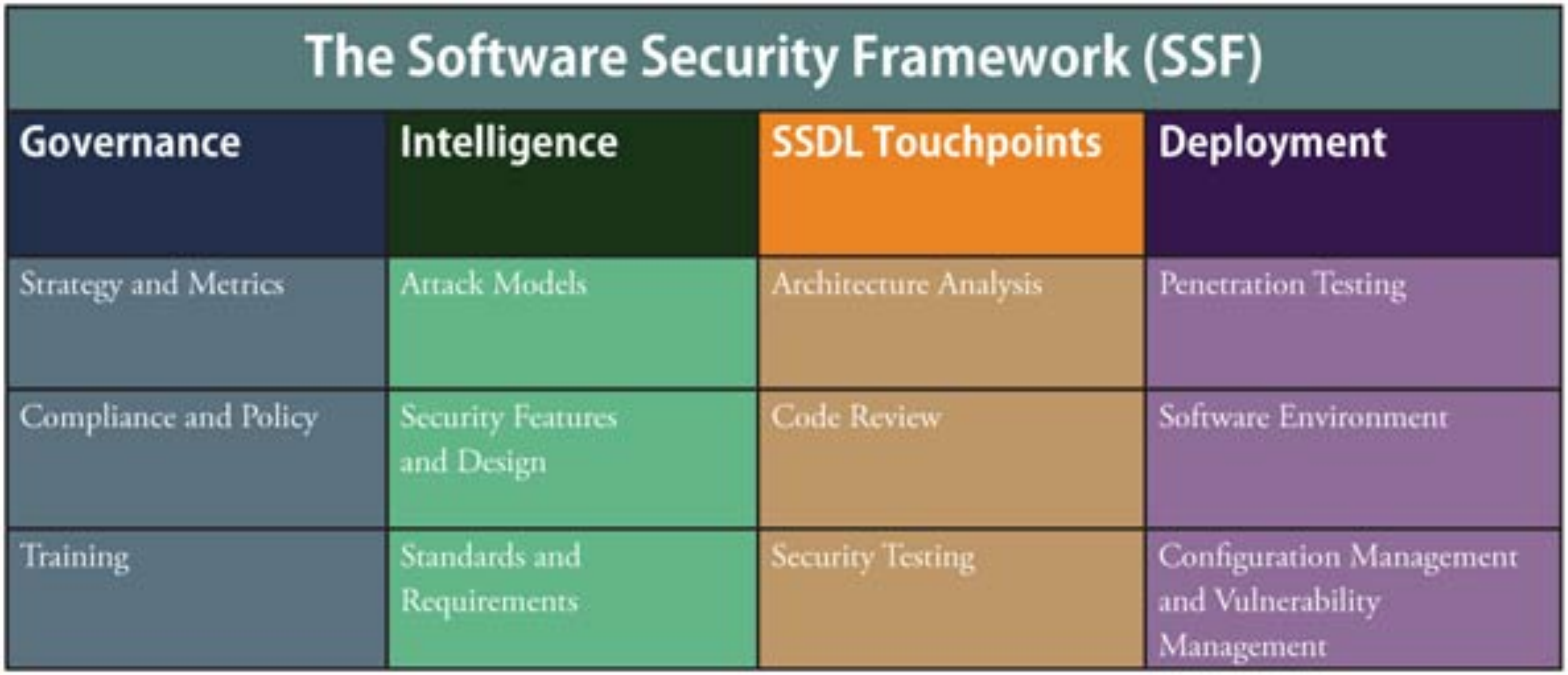
Source: https://msdn.microsoft.com/en-us/library/windows/desktop/cc307406.aspx



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

BUILT-IN SECURITY MATURITY MODEL - BISMM

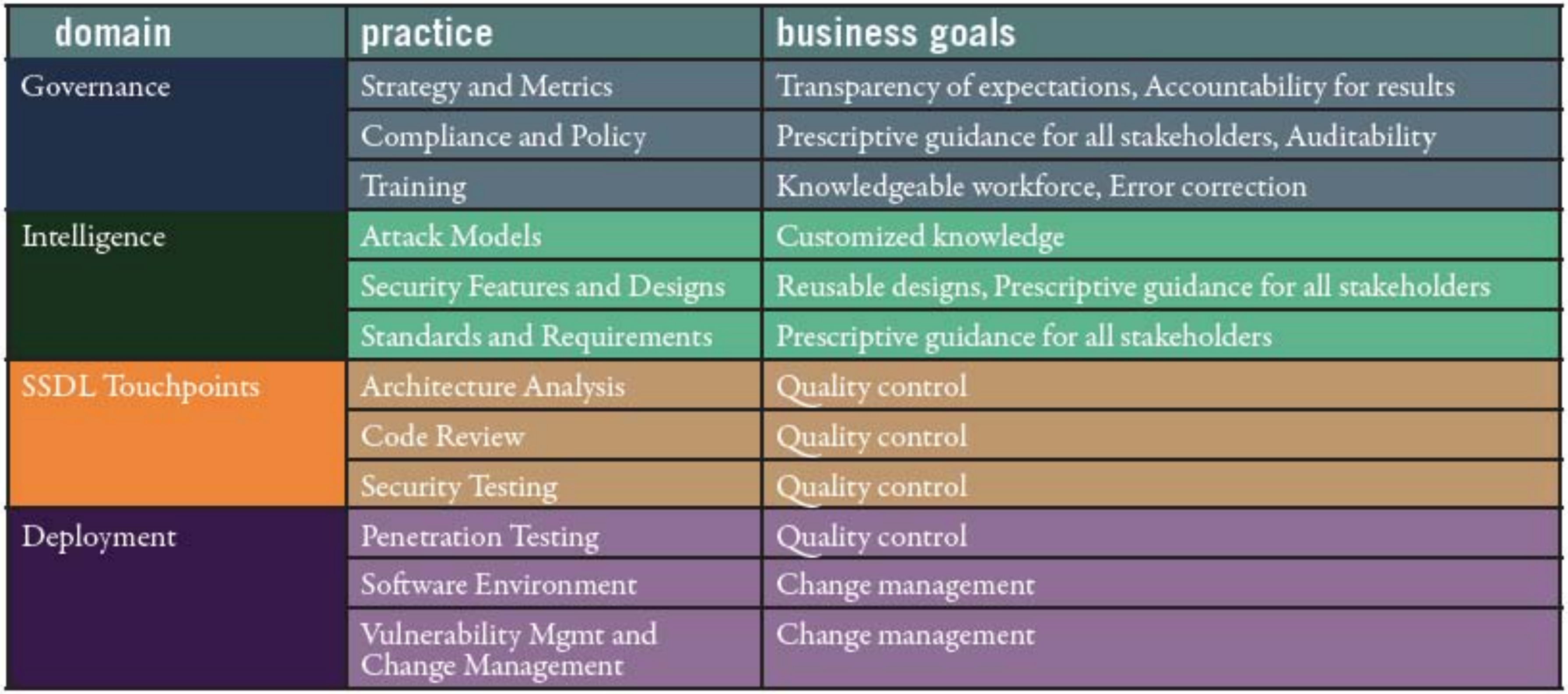


The Software Security Framework (SSF)

Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

https://www.bsimm.com/

HOW THE BISMM TRANSLATES TO BUSINESS GOALS



domain	practice	business goals
Governance	Strategy and Metrics	Transparency of expectations, Accountability for results
	Compliance and Policy	Prescriptive guidance for all stakeholders, Auditability
	Training	Knowledgeable workforce, Error correction
Intelligence	Attack Models	Customized knowledge
	Security Features and Designs	Reusable designs, Prescriptive guidance for all stakeholders
	Standards and Requirements	Prescriptive guidance for all stakeholders
SSDL Touchpoints	Architecture Analysis	Quality control
	Code Review	Quality control
	Security Testing	Quality control
Deployment	Penetration Testing	Quality control
	Software Environment	Change management
	Vulnerability Mgmt and Change Management	Change management

WHAT CAN WE CONCLUDE?

- **Security frameworks and lifecycles can vary greatly.**
- **Alignment with the overall software development approach in an organization is needed – if it is known and/or followed.**
  - Observation: Most organizations struggle with software lifecycles in general.
- **These frameworks and lifecycle models may need adaptation to adequately include security testing.**

THE TYPICAL IT SECURITY VIEW OF SECURITY TESTING

- **Generally, limited to penetration testing**
  - Perhaps also “bug bounties” and incident response testing
- **Very little mention of functional security testing.**

PENETRATION ("PEN") TESTING

- **Is needed and is helpful**
- **But…**
  - It is a snapshot
  - Follows the "event" model and typically can't be sustained
  - Lacks the internal view of security

THERE ARE NO EASY ANSWERS

- There is no single solution.
- However, it is clear we can and must do better in safeguarding valuable physical and digital assets.
- It’s like Y2K without the deadline!

WHAT IS NEEDED?

- **A holistic approach that involves software testers, with security testing as a priority in all project activities.**
  - Continuous security testing in all forms
- **Strong executive leadership.**
  - Board presence is needed
  - Independence is needed
  - The CISO may not be independent enough for board-level accountability
- **Complete organizational compliance**

TANGIBLE STEPS

- **Raise awareness at all levels**
  - Not just that “cybersecurity is important”
  - But, we are not doing nearly enough to stay even close to vigilant
- **Assess risks and threats continuously**
- **Get training**
  - The ISTQB Advanced Security Tester certification is a great start
- **Build your framework – soon**
  - You don’t have to start from scratch

RESOURCES

- **ISTQB Security Tester Syllabus**
  - https://www.astqb.org/documents/Advanced-Security-Tester-Syllabus-GA-2016.pdf
- **NIST Publications**
  - https://www.nist.gov/publications
  - Search for “cybersecurity”

BOOKS

- **Hacking: The Art of Exploitation, 2nd Edition 2nd Edition**
  - Jon Erickson
- **Fuzzing: Brute Force Vulnerability Discovery 1st Edition**
  - Sutton, Green, Amini
- **The Art of Deception**
  - Kevin Mitnick
- **The Art of the Steal**
  - Frank Abagnale

TRAINING

- **Rice Consulting's Foundational Security Testing Methods Course**
  - http://bit.ly/2lmopTy
- **ISTQB Advanced Security Testing Course**
  - http://bit.ly/2lsUaaq
  - https://www.mysoftwaretesting.com/category_s/60.htm
  - E-Learning available
  - Public course – March 7 – 10, 2017, Irving, TX
  - Coming in May to the Salt Lake City area
  - Looking for suggestions of other locations

RECORDING AND NOTES

- http://randallrice.blogspot.com
- About 30 minutes after the session.

YOUR QUESTIONS?

RICE CONSULTING

thank you

BIO - RANDALL W. RICE

- Over 35 years experience in building and testing information systems in a variety of industries and technical environments
- ISTQB Certified Tester – Foundation level (CTFL), Advanced Level (CTAL) Full, Advanced Security Tester (CTAL-SEC)
- ASTQB Certified Mobile Tester (CMT)
- ISTQB Foundation Level Agile Tester (CTFL-AT)
- Director, American Software Testing Qualification Board (ASTQB)
- Chairperson, 1995 - 2000 QAI's annual software testing conference
- Co-author with William E. Perry, *Surviving the Top Ten Challenges of Software Testing* and *Testing Dirty Systems*
- Principal Consultant and Trainer, Rice Consulting Services, Inc.

RICECONSULTING

CONTACT INFORMATION

Randall W. Rice, CTAL

Rice Consulting Services, Inc.

1608 SW 113th Pl

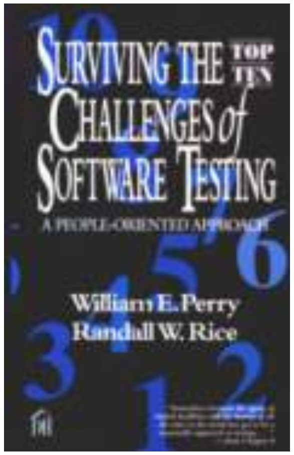
Oklahoma City, OK 73170

Ph: 405-691-8075

Fax: 405-691-1441

Web site: www.riceconsulting.com

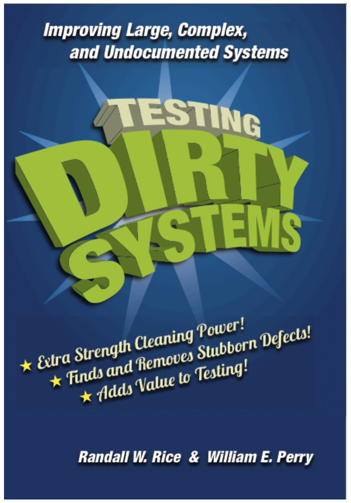
e-mail: rrice@riceconsulting.com



SURVIVING THE TOP TEN CHALLENGES of SOFTWARE TESTING

A PEOPLE-ORIENTED APPROACH

William E. Perry
Randall W. Rice



Improving Large, Complex, and Undocumented Systems

TESTING DIRTY SYSTEMS

★ Extra Strength Cleaning Power!
★ Finds and Removes Stubborn Defects!
★ Adds Value to Testing!

Randall W. Rice & William E. Perry

RICECONSULTING