CYBERSECURITY AND THE ACCOUNTABILITY OF ELECTED OFFICIALS

2014 NACo National Cyber Symposium

April 10, 2014

NACo CYBER for COUNTIES

An initiative of the National Association of Counties

RALPH JOHNSON, CISSP, HISP, CISM, CIPP/US

Chief Information Security and Privacy Officer – King County Washington

Governance Board President – Holistic Information Security Practitioner Institute (HISPI)

Member – ITT Technical Institute – Seattle, Program Advisory Council

Member – MS-ISAC Trusted Purchasing Alliance Product Review Board

Member – MS-ISAC Education and Awareness Committee

Member – National Association of Counties (Naco) Cyber-Security Task Force

King County Information TECHNOLOGY

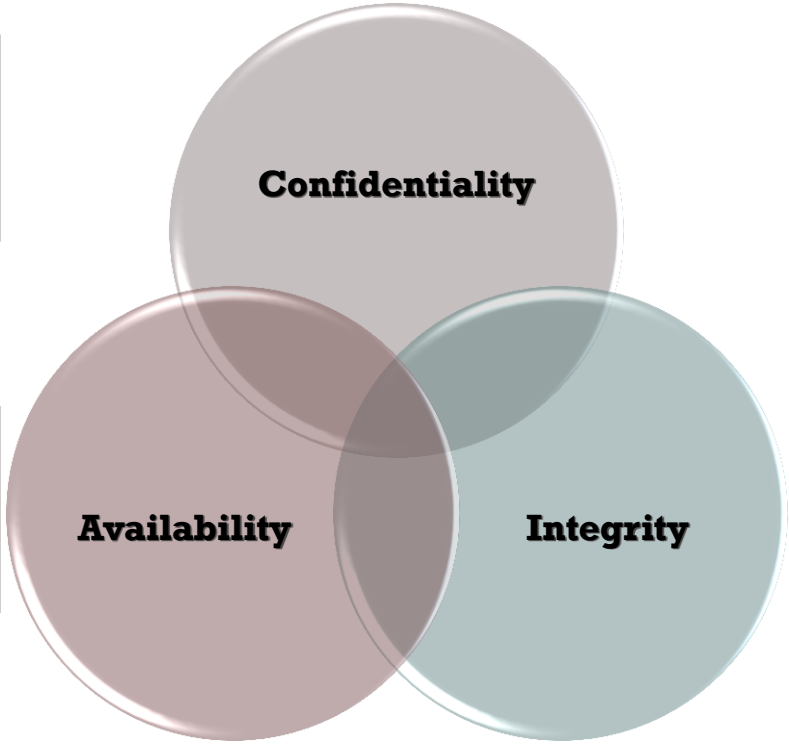
HOLISTIC INFORMATION SECURITY PRACTITIONER INSTITUTE HISPI

A loss of *confidentiality* results in the unauthorized disclosure of information

A loss of *availability* results in disruption of access to or use of information or an information system

A loss of *integrity* results in the unauthorized modification or destruction of information

INFORMATION SECURITY MANAGES RISK RELATED TO CONFIDENTIALITY, AVAILABILITY, AND INTEGRITY OF INFORMATION AND RELATED ASSETS AND DELIVERY SYSTEMS.



WHO IS ULTIMATELY RESPONSIBLE FOR INFORMATION SECURITY?

Information Security is an organizational issue

Everyone

INFORMATION ASSURANCE AND PUBLIC DISCLOSURE

Governments have a duty of care to protect information with which it is entrusted from unauthorized disclosure, modification and/or destruction.

Protection does not mean "unavailable to the public when necessary".

US BREACH STATISTICS 2005 - PRESENT

All Sectors

Breaches – 4,239

Records – 864,108,052

Government

Breaches – 678 (15.9%)

Records – 148,366,723 (17.2%)

LUCIE F. HUGER, ESQUIRE

Officer – Greensfelder, Hemker & Gale P.C.

GREENSFELDER
ATTORNEYS AT LAW

DATA MAINTAINED/ STORED/ COLLECTED IS DATA AT RISK

Examples of Personally Identifiable Information Maintained by County Governments:

- **Tax Records**
- **Payroll, Benefit and Retirement information of Public Employees**
- **Information about public school students**
- **Court Records**
- **Criminal Records**
- **Information relating to medical programs**
- **Information relating to social services**

DATA IS EVERYWHERE

With the popularity of social media; conducting business on personal devices; and outsourcing certain business functions to third parties, data breaches are becoming more prevalent.

POSSIBLE OUTCOMES AFFECTING COUNTY OPERATIONS RESULTING FROM A BREACH

- Political Fallout
- Damage to reputation
- Compliance obligations
- Federal investigations
- Investigations by State Attorney General
- Possible Civil litigation

COMMON CAUSES OF DATA BREACHES

Negligence

Malicious or criminal attacks (hacking or theft of electronic devices)

Employee/Contractor malfeasance

LIABILITIES

County governments and county officials are not exempted from compliance with applicable laws aimed at protecting personally identifiable information and may be subject to penalties and fines.

Depending upon the laws of the particular State, sovereign immunity may protect county governments and county officials from tort liabilities arising out of failing to comply with applicable laws aimed at protecting personally identifiable information.

RECENT CASES IN THE NEWS

Skagit County, WA

Los Angeles County, CA

Monterey County, CA

Erie County, NY

Harris County, TX

IN THE EVENT OF A DATA BREACH

Notify those within the organization of the incident who need to know

Assemble a response team of both internal stakeholders and external experts

Carefully investigate and keep language of the investigation in language that is easy to understand

Determine whether the incident constitutes a reportable breach: Federal laws and 46 different state laws

Contain the breach and mitigate the harm, to the extent possible

Notify persons impacted

Respond to inquiries

Improve processes

PROACTIVE APPROACH

Create a Preparedness Plan, now:

Identify persons within your organization who are/will be responsible for data management.

Identify compliance requirements according to applicable laws.

Identify the types of data your organization collects/ processes/ develops.

Create a risk assessment plan and mitigation plan.

Develop policies and educate all staff.

Have a reporting mechanism that is well publicized and encouraged.

Review vendor contracts.

Contact Information

Lucie F. Huger
314/345-4725
E-mail: lfh@greensfelder.com

GREENSFELDER
ATTORNEYS AT LAW

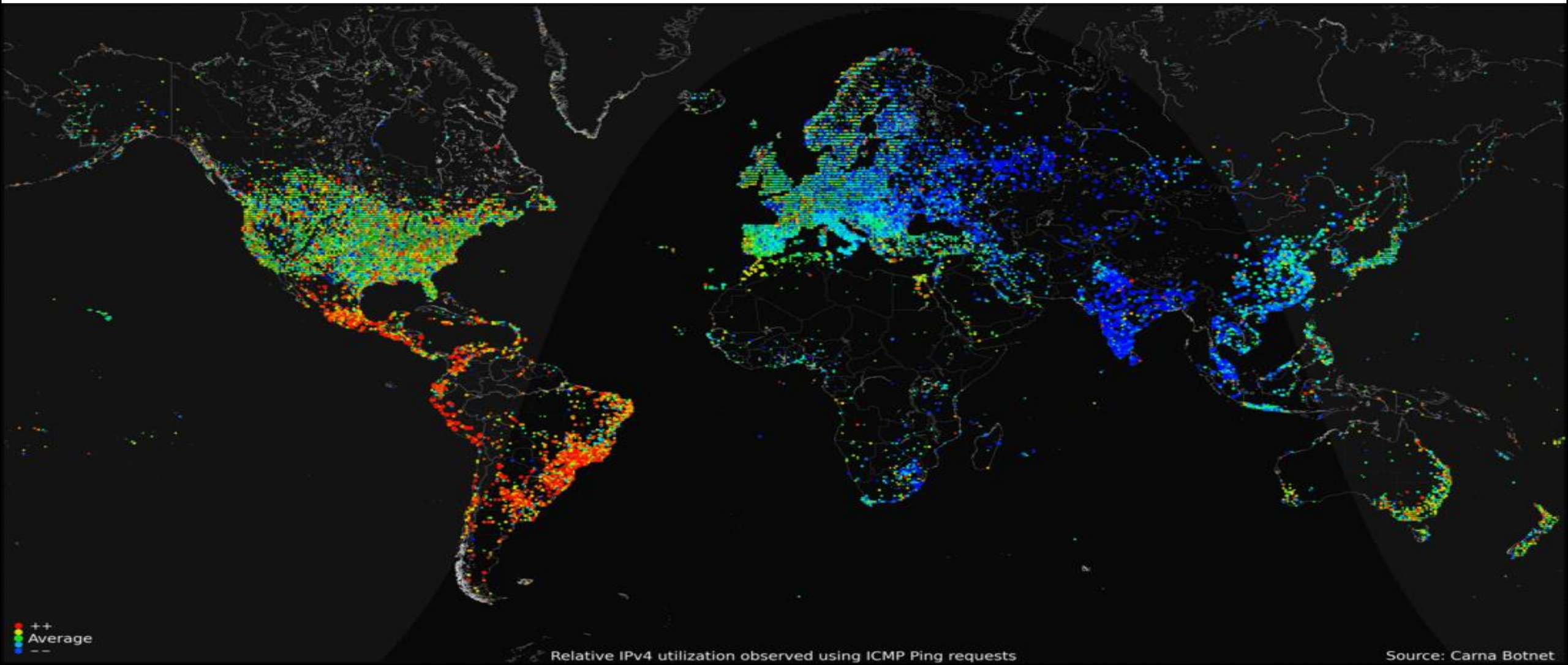
ANDREW DOLAN

Director of Government Affairs – Multi-State Information Sharing and Analysis Center

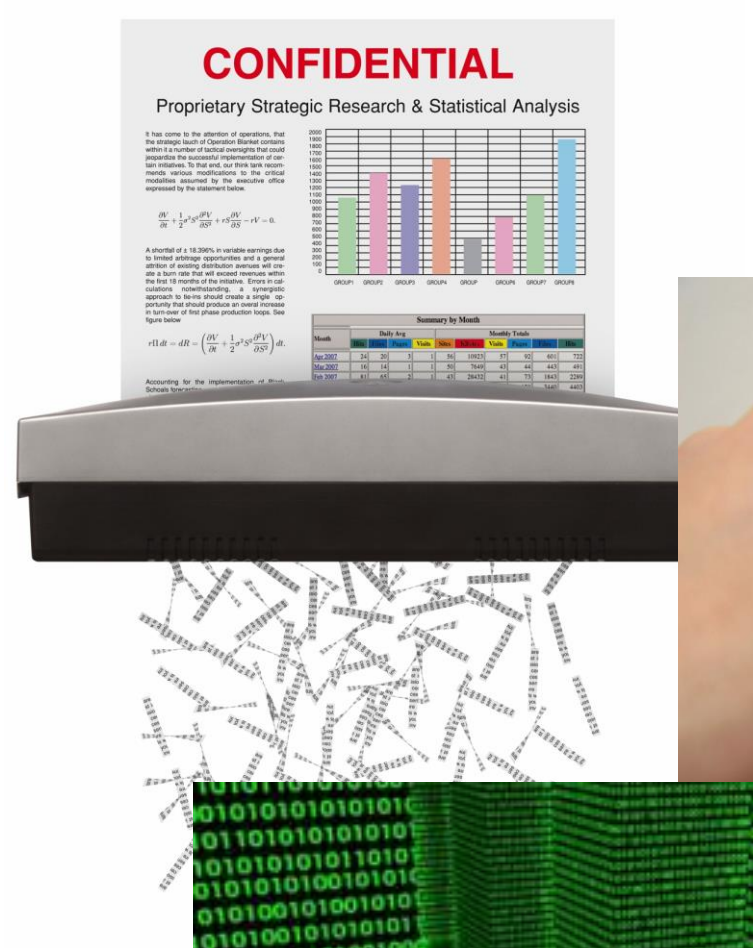
Center for Internet Security – CEO: Will Pelgrin

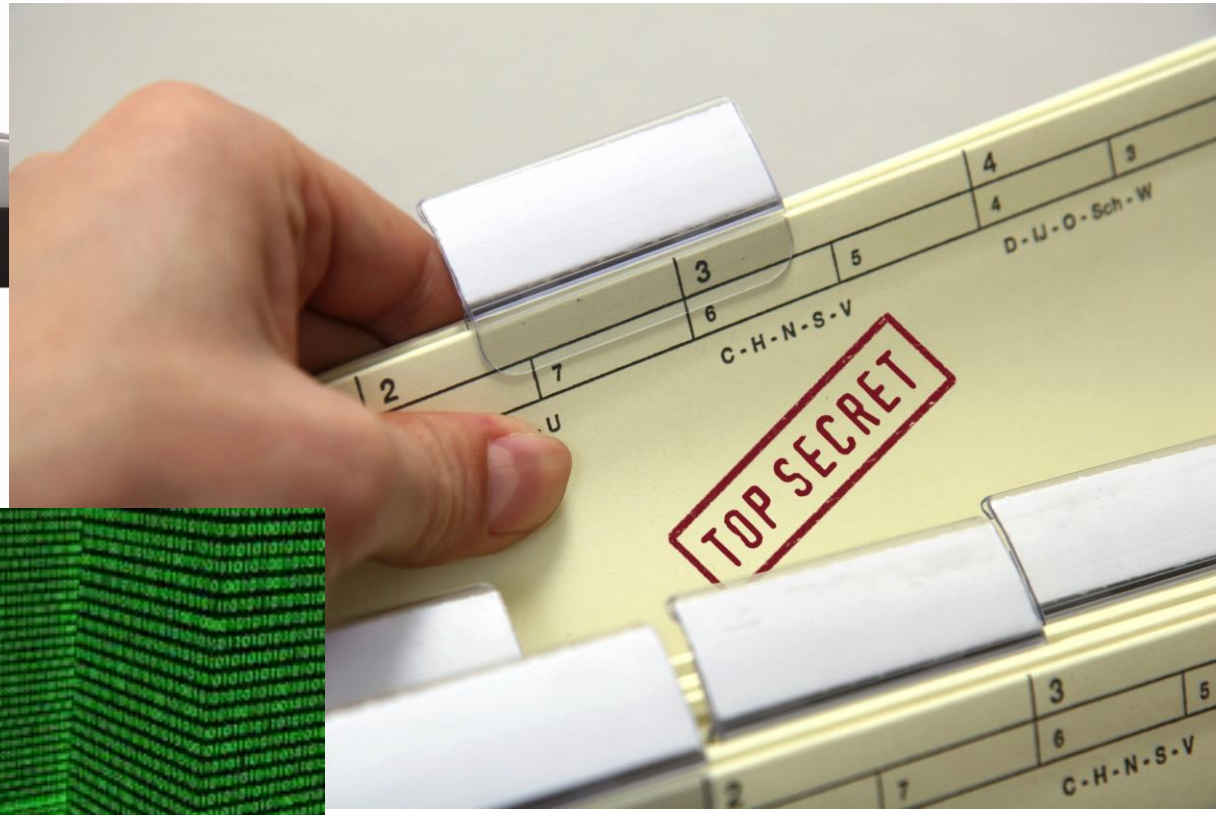
CENTER FOR INTERNET SECURITY®

THE INTERNET



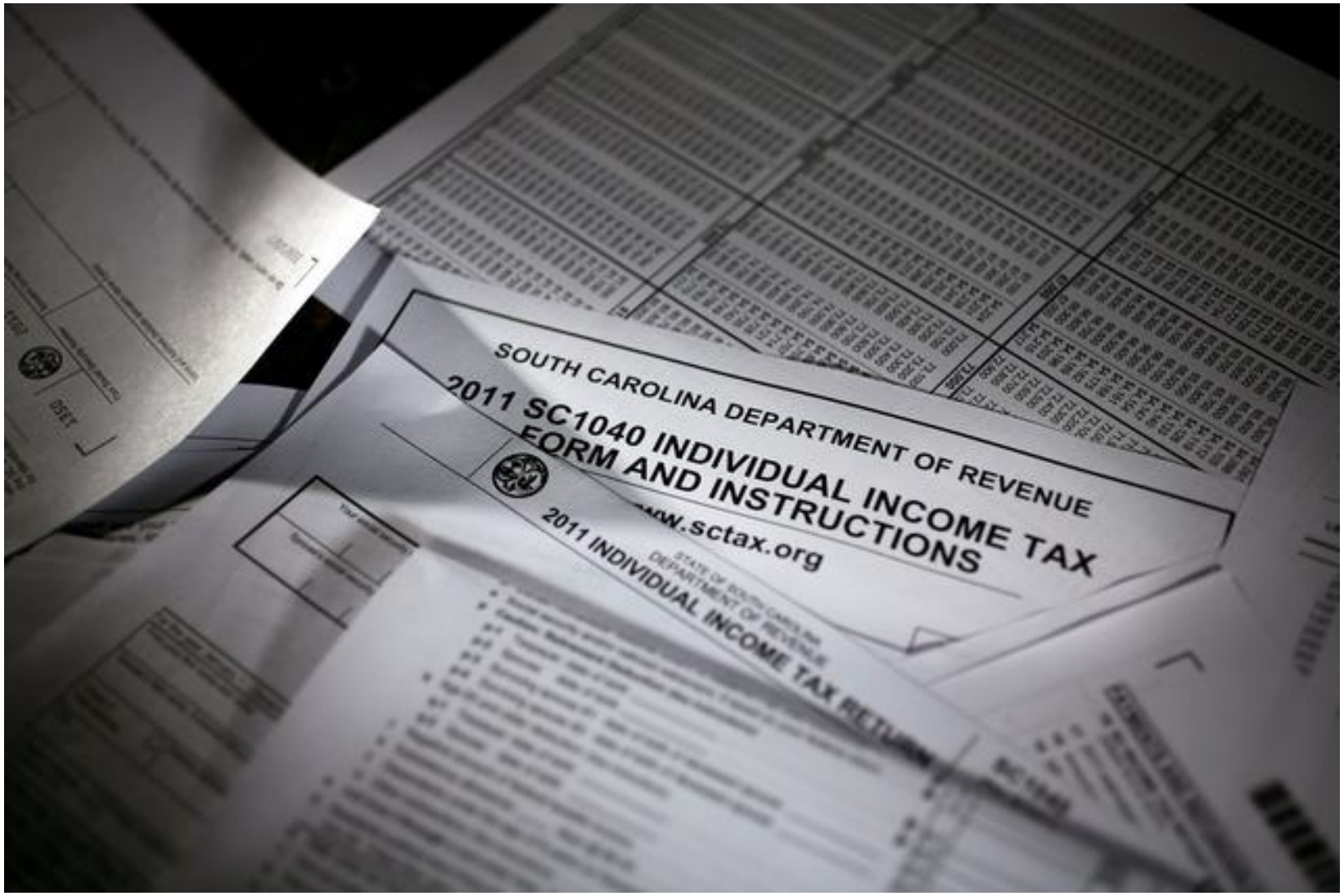
CRIMINALS LOOK FOR DATA...






MALWARE
WORM
SPAM
TROJANHORSE
VIRUS
SPYWARE
PHISHING

SOUTH CAROLINA



EMERGENCY ALERT SYSTEMS COMPROMISED

'Hackers' access Emergency Alert System of local Great Falls, Montana TV station to broadcast fake warning of 'Zombie Apocalypse'

Time Newsfeed
Tue, 12 Feb 2013 14:33 CST

A Montana television station's regular programming was interrupted by news of a zombie apocalypse.

The Montana Television Network says hackers broke into the Emergency Alert System of Great Falls affiliate KRTV and its CW station Monday.

KRTV says on its website the hackers broadcast that "dead bodies are rising from their graves" in several Montana counties.

The alert claimed the bodies were "attacking the living" and warned people not to "approach or apprehend these bodies as they are extremely dangerous."

The network says there is no emergency and its engineers are investigating.

A call to KRTV was referred to a Montana Television Network executive in Bozeman. Jon Saunders didn't immediately return a call for comment.

WHAT CAN YOU DO?

BE PROACTIVE!

Leadership

Governance

Responsibility (Assign)

Compliance (Measure)

THERE'S NO SUCH THING AS 100% CYBER SECURITY...

Harden systems

Keep your systems patched

Update cyber security policies

Monitor compliance with the policies

Regularly scan systems

Backup your systems on a regular basis and store off site

Encrypt your mobile devices

Train your users

CIS CAN HELP!

CENTER FOR INTERNET SECURITY®

Resources

- Daily tips
- Monthly newsletters
- Webcasts
- Guides
- Nationwide Cyber Security Review (NCSR)
- 24x7 Managed/Monitored Security Services
- Vulnerability Assessments
- Penetration Testing

www.cisecurity.org

Contact Information

Andrew.Dolan@cisecurity.org

or

info@msisac.org

www.cisecurity.org

518-880-0699

GOPAL KHANNA

Managing Partner – The Khanna Group, LLC

Transformation by Design®

The Khanna Group

TRANSFORMATION BY DESIGN

Action to Direction

Implementation to Execution

Destruction to Construction

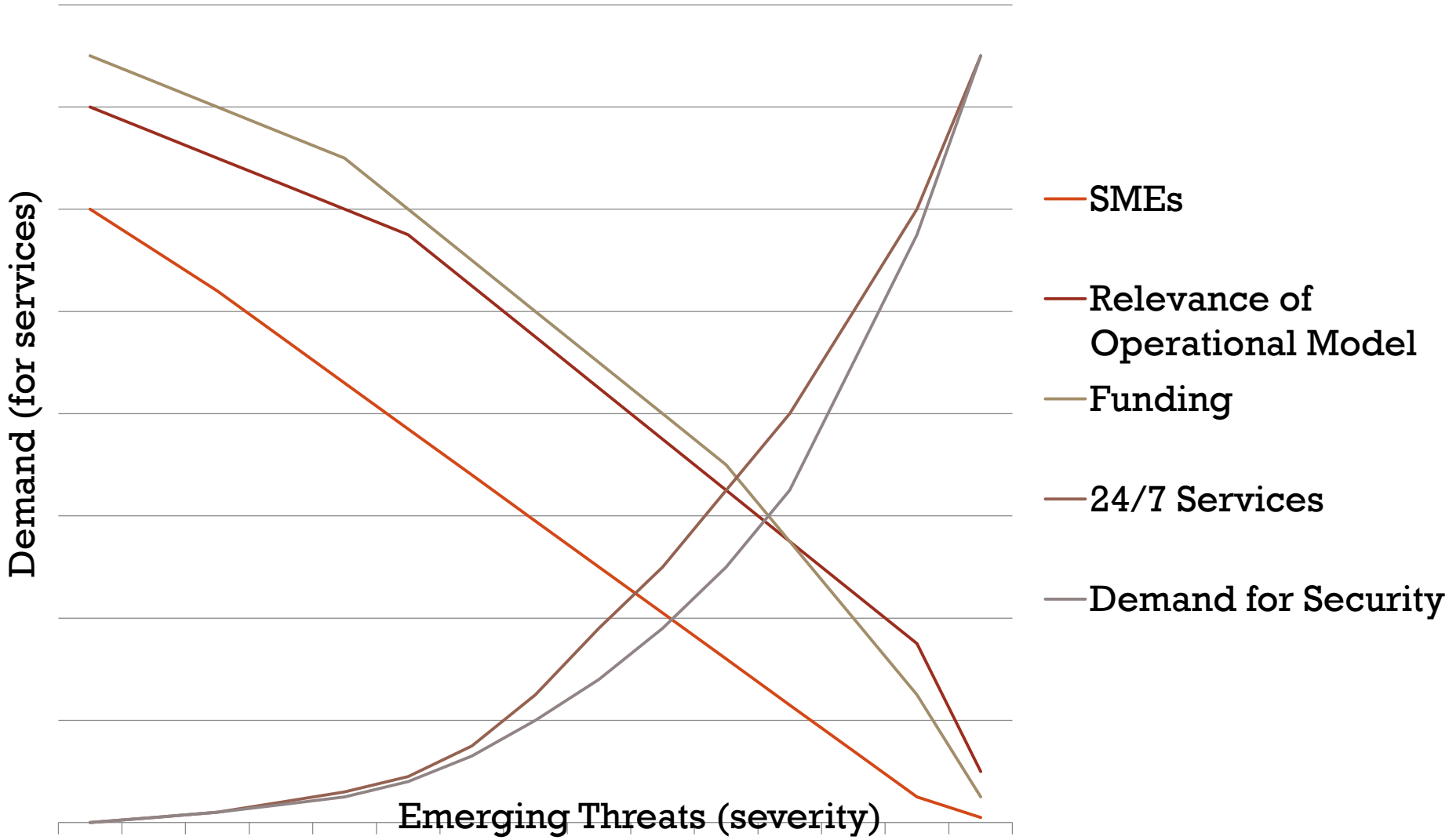
PARADIGM SHIFT

Board of Directors vs. Elected Officials

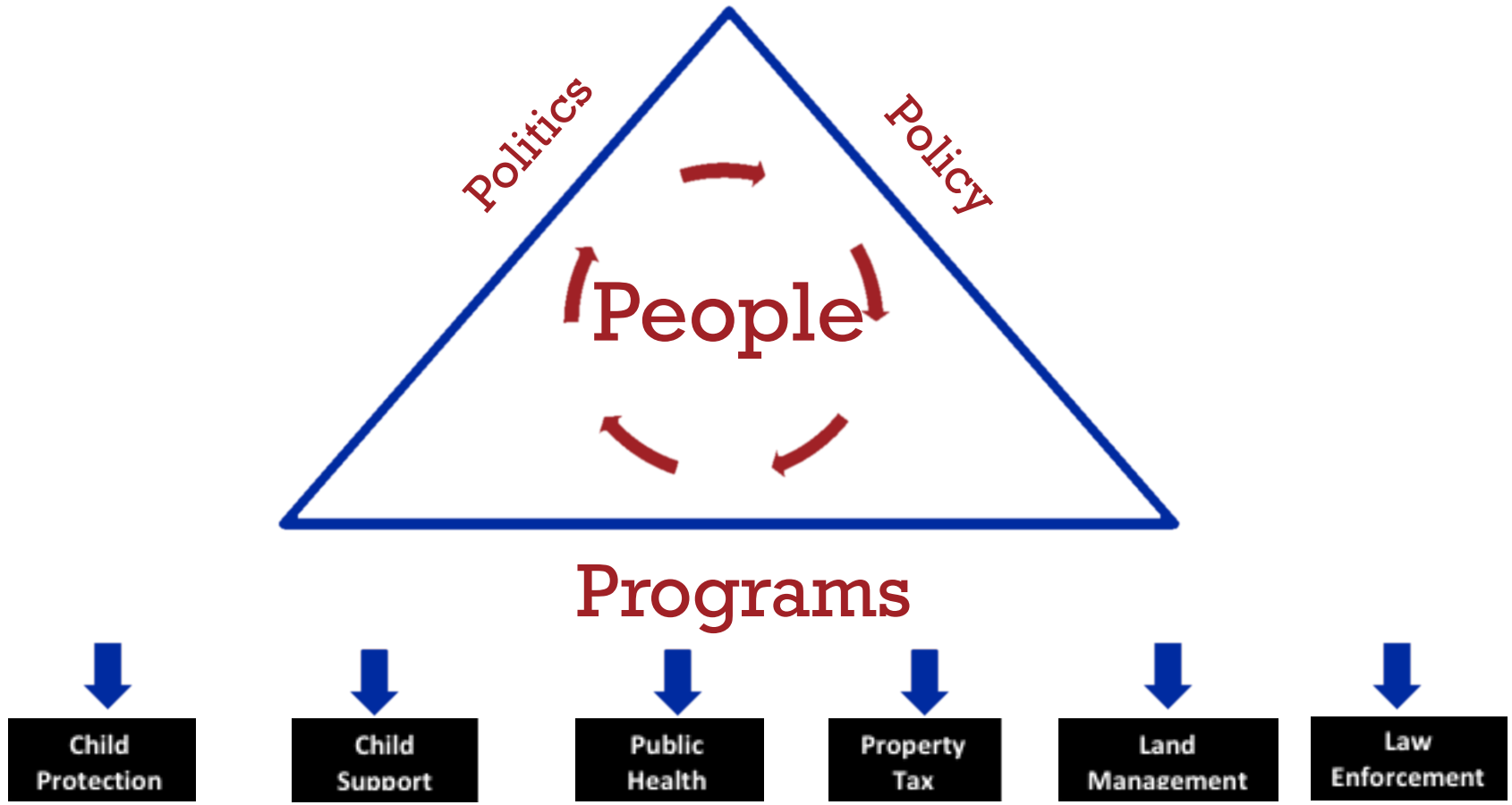
Executive Team vs. Administrators/Managers

Subject Matter Experts vs. Staff/Employees

DEMAND FOR SERVICES AS NEW THREATS EMERGE



GOVERNMENT IS "BROKEN"

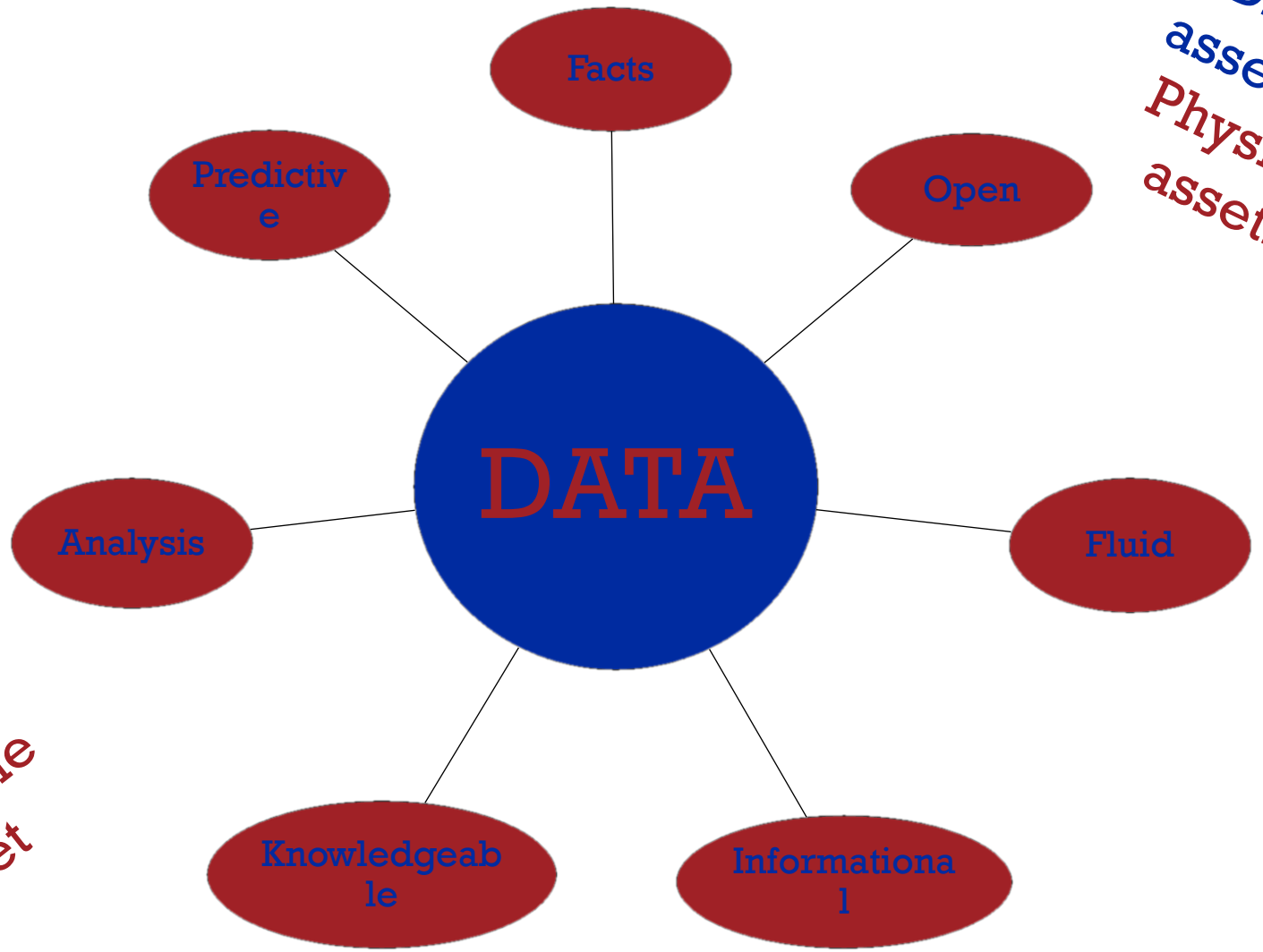


Government **WORKS**

CYBER SECURITY IS ABOUT PROTECTING DATA

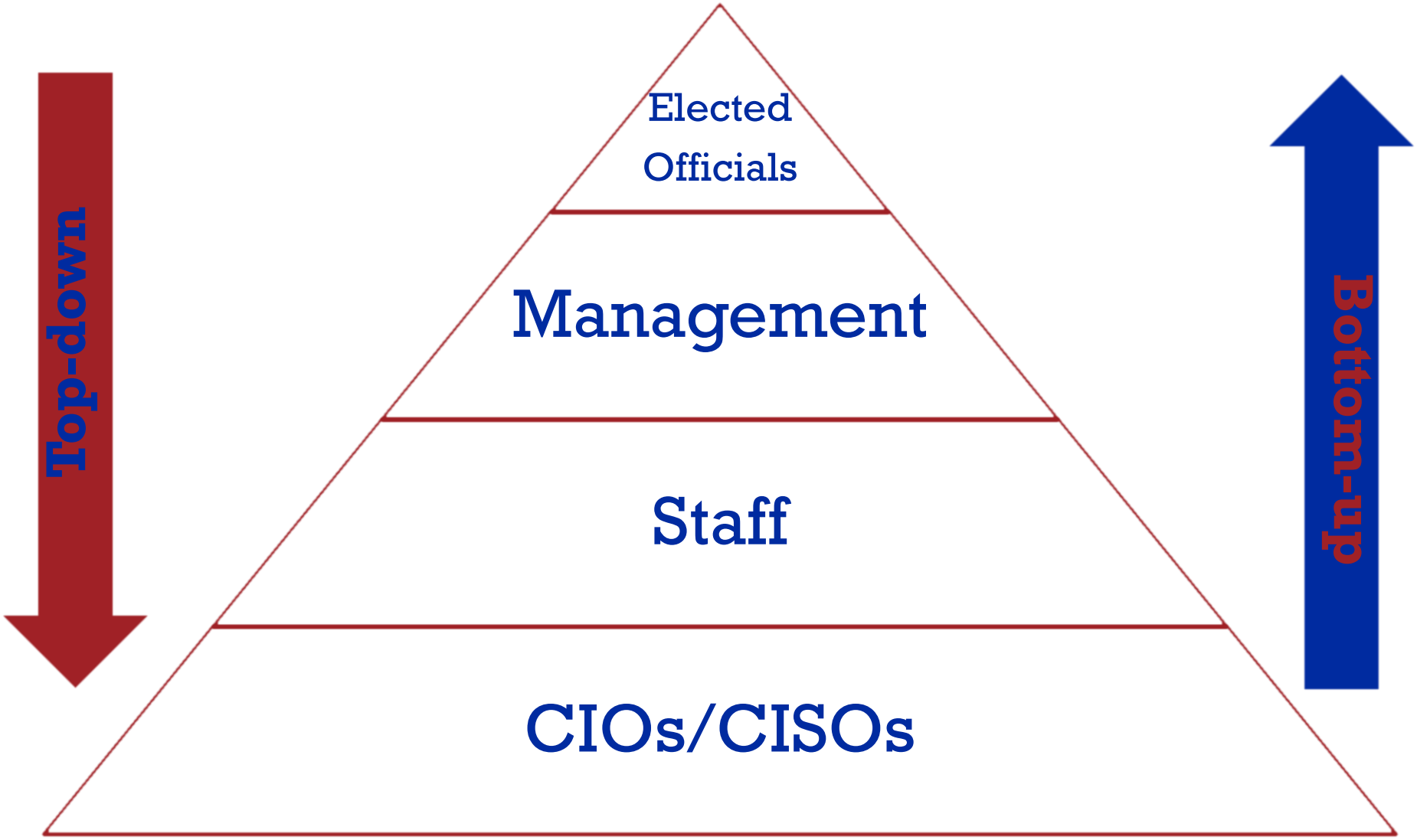
Data is King

Digital assets vs. Physical assets

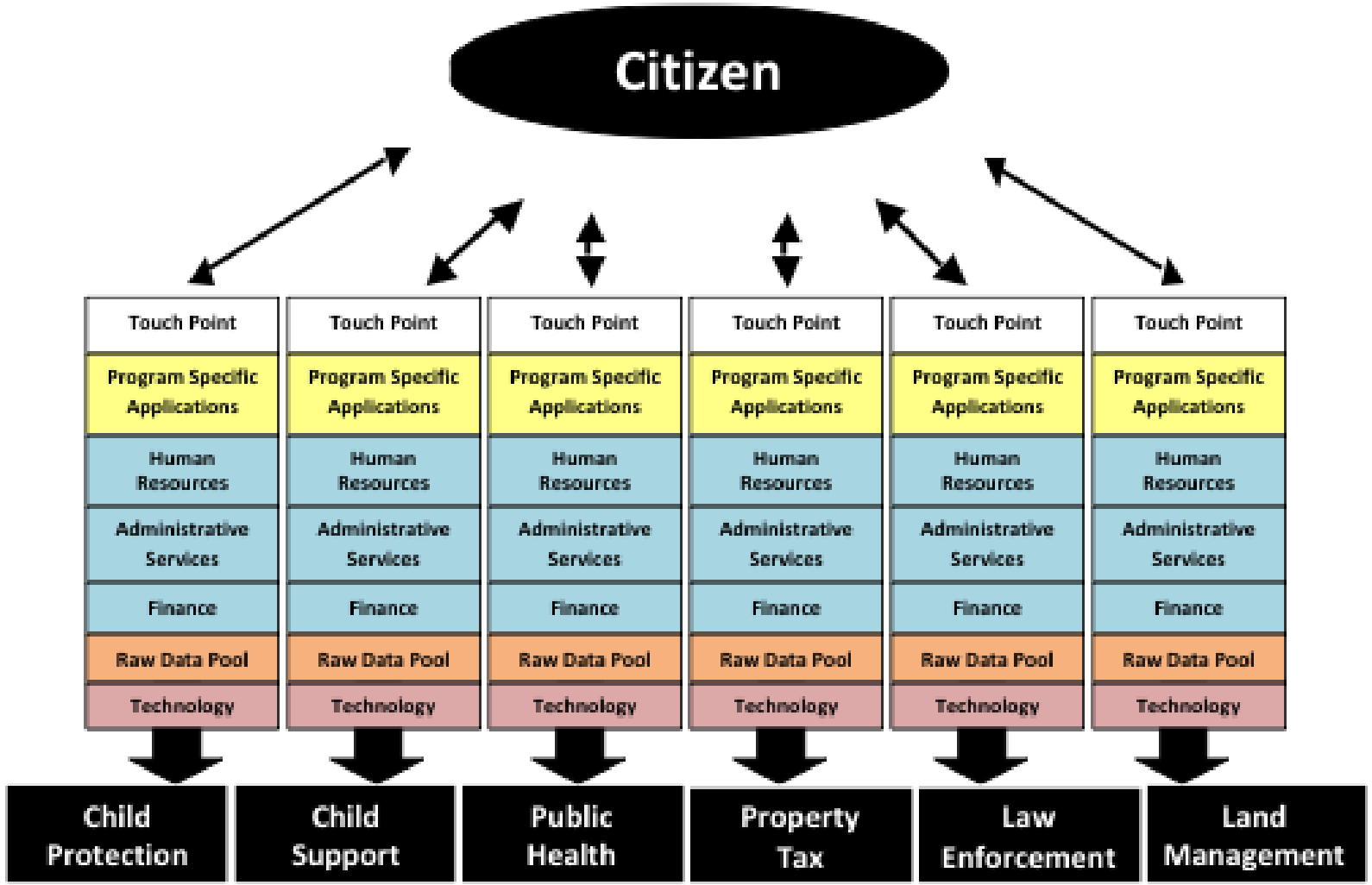


Data=Most Valuable asset

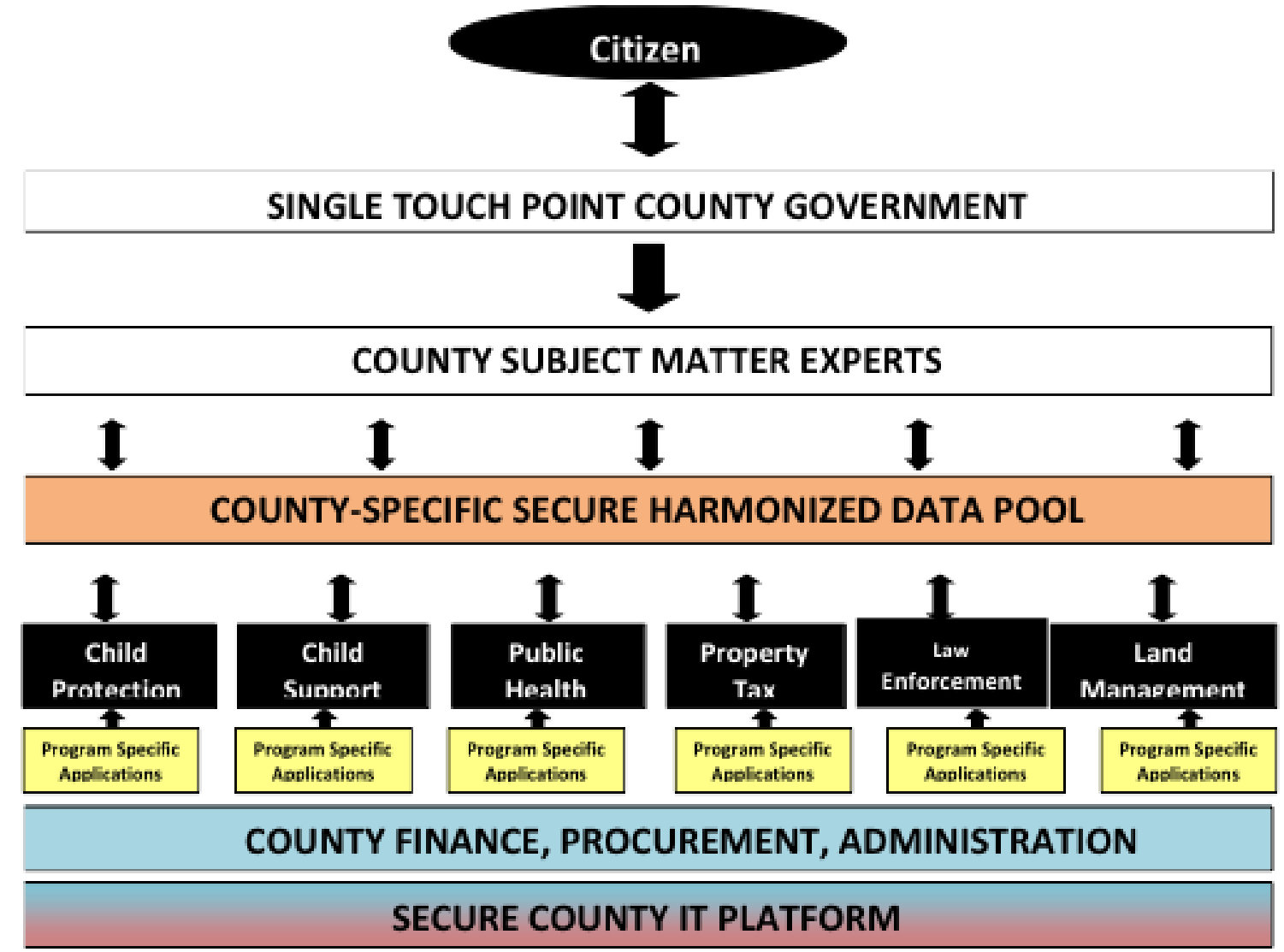
BRIDGING ELECTED OFFICIAL & CIO DISCONNECT



Current State: Program-Centric Services Model



Future State: Citizen-Centric Services Model



TRANSFORMATION BY DESIGN

Action to Direction

Implementation to Execution

Destruction to Construction

ACTION TO DIRECTION

Allow fiscal flexibility

Bi-partisan agreement

Clear mission

Devoid of "big P" and "small p"

Long term security

Partner with Unions

Operational re-design

Institutionalize support

Eliminate fear of failure

Staffing flexibility

Security part of job description

Secure public Data and information

IMPLEMENTATION TO EXECUTION

Empower SMEs by :

- Tolerating risk, allow pivoting
- Encouraging curiosity, providing incentives
- Bottom-up change, let SMEs redesign processes
- Accept recommendation from SMEs
- Avoid "Analysis Paralysis"
- Providing direction, clarity of objective
- 80/20 rule

DESTRUCTION TO CONSTRUCTION

Enterprise view

Horizontal approach

Destroy silos

Start small-build scale

Give up the old, create the new

Leave legacy

Distribute knowledge

Give up control

Collaborate

Reporting

Accept opinion

Re-design vs. incremental

Re-purpose resources

Comprehensive sharing

Contact Information

Gopal Khanna

gopal.khanna@gmail.com

952-484-5123

"Transformation by Design"

Gopal Khanna

The Khanna Group

CONTACT INFORMATION

Ralph Johnson, CISSP, HISP, CISM, CIPP/US
ralph.Johnson@kingcounty.gov
(206) 263-7891

Lucie F. Huger, Esquire
(314) 345-4725
lfh@greensfelder.com

Andrew Dolan
andrew.dolan@cisecurity.org
(518) 880-0699

Gopal Khanna
gopal.khanna@gmail.com
952-484-5123