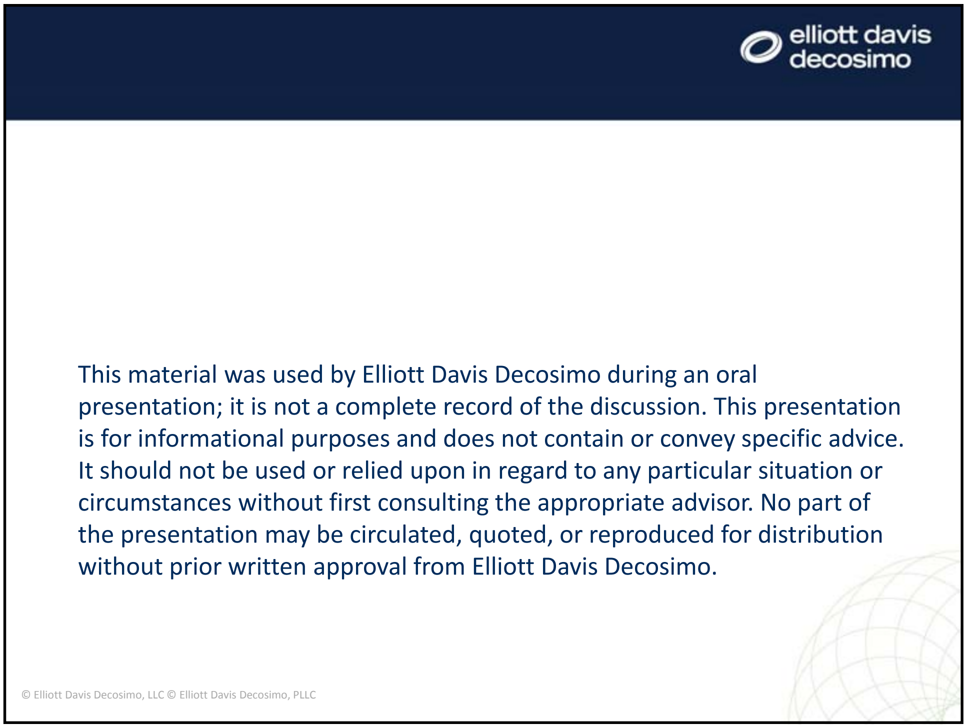
Cybersecurity Update - State and Local Governments and Related Entities

Bonnie Bastow
Director – Risk Advisory Services
bonnie.bastow@elliottdavis.com
704.808.5275

Fellen Yang
Manager – Risk Advisory Services
fellen.yang@elliottdavis.com
704.808.5290

June 14, 2017



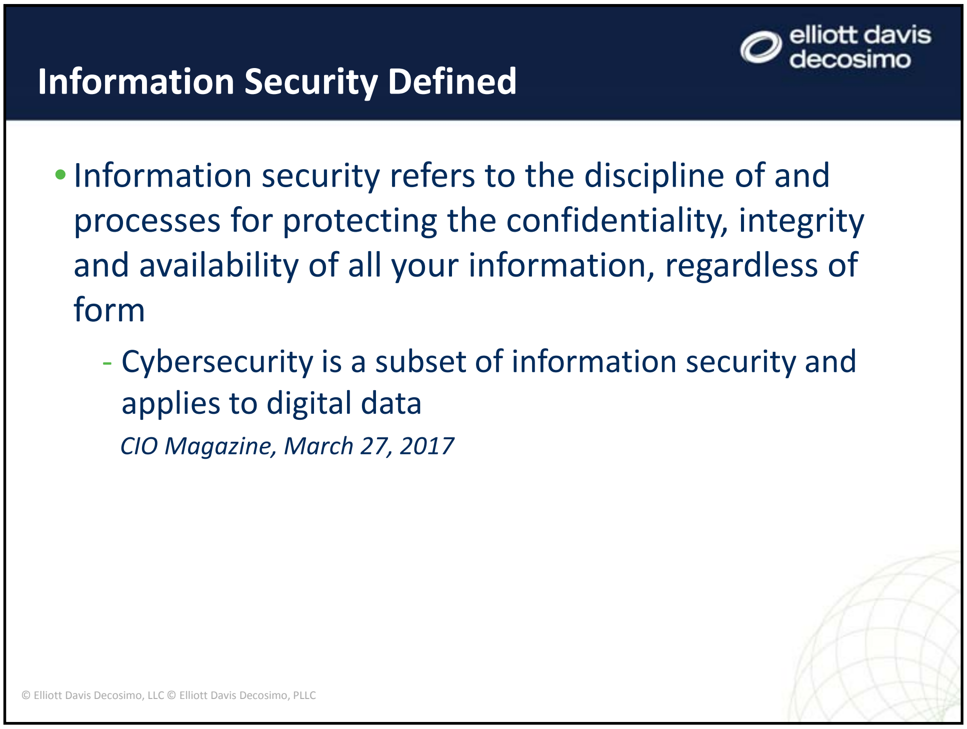
This material was used by Elliott Davis Decosimo during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon in regard to any particular situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis Decosimo.

Agenda

1. Cybersecurity Defined, Background And Risks
2. Resources Available
3. Recommendations
4. Latest Update on Cybersecurity Risk

Cybersecurity Defined, Background And Risks Agenda Item # 1

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
Klossner



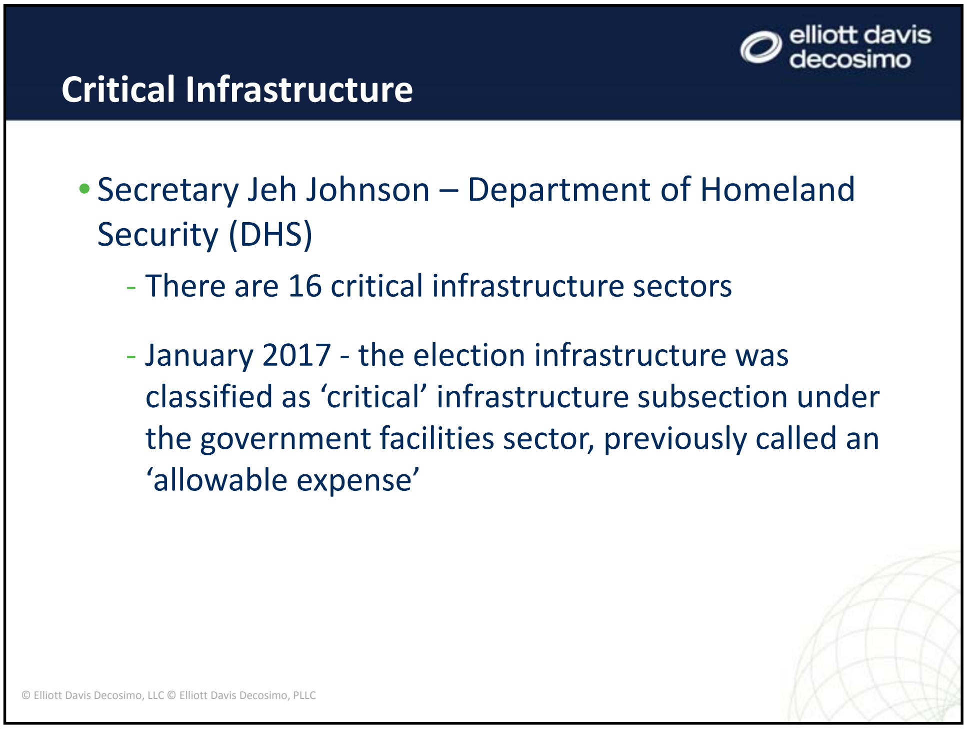
Information Security Defined

- Information security refers to the discipline of and processes for protecting the confidentiality, integrity and availability of all your information, regardless of form
  - Cybersecurity is a subset of information security and applies to digital data

    CIO Magazine, March 27, 2017

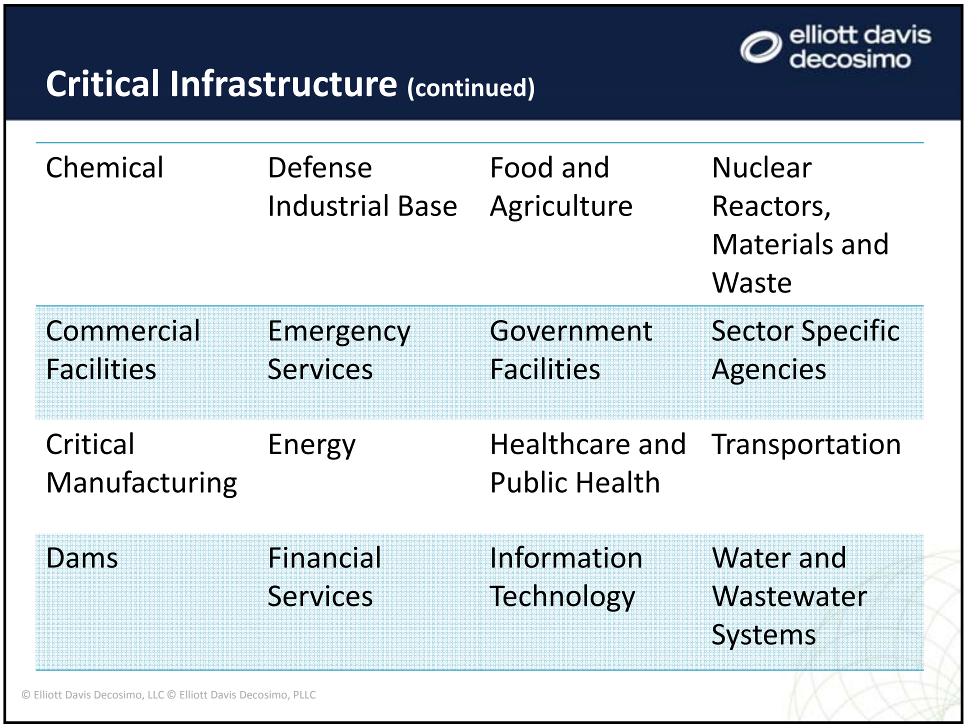
Cybersecurity Defined

Cybersecurity are the efforts and resources deployed by an organization to protect its digital information assets.



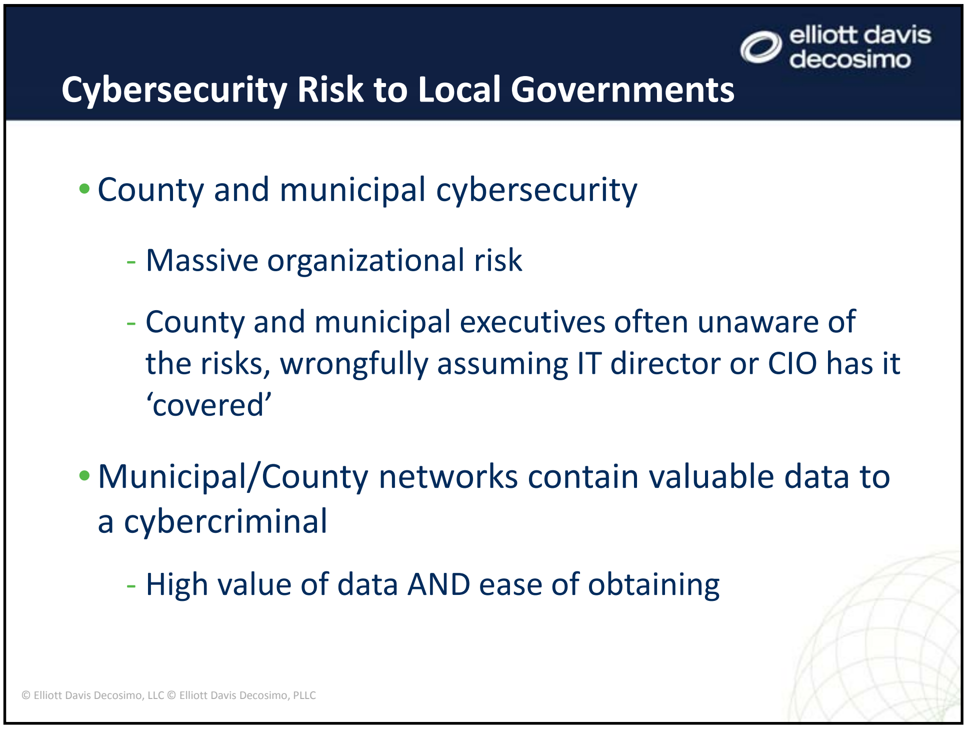
Critical Infrastructure

- Secretary Jeh Johnson – Department of Homeland Security (DHS)
  - There are 16 critical infrastructure sectors
  - January 2017 - the election infrastructure was classified as ‘critical’ infrastructure subsection under the government facilities sector, previously called an ‘allowable expense’



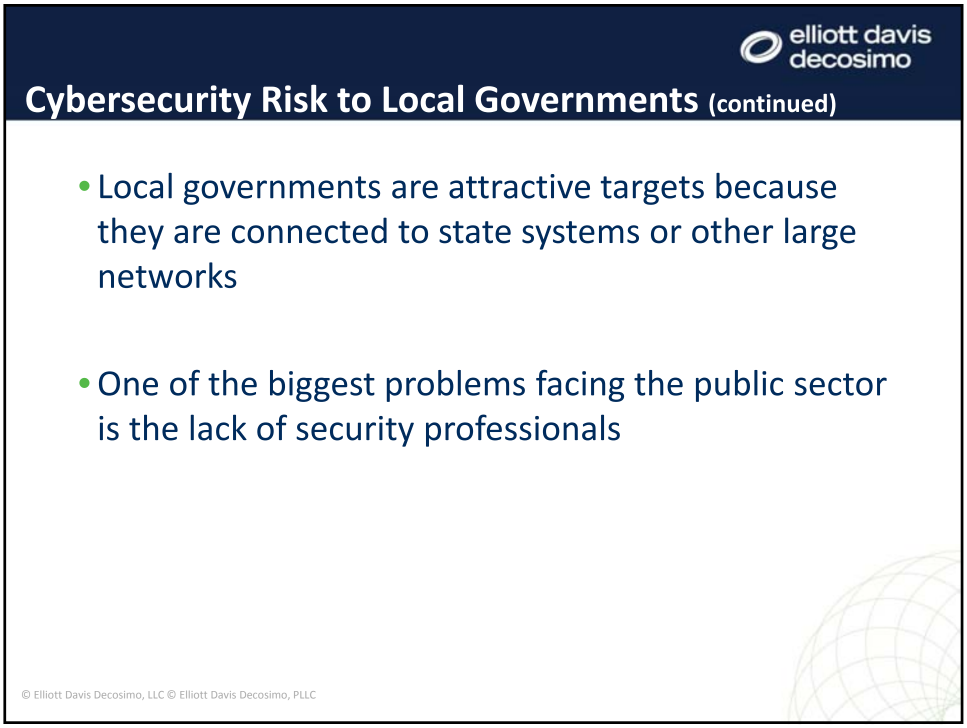
Critical Infrastructure (continued)

Chemical	Defense Industrial Base	Food and Agriculture	Nuclear Reactors, Materials and Waste
Commercial Facilities	Emergency Services	Government Facilities	Sector Specific Agencies
Critical Manufacturing	Energy	Healthcare and Public Health	Transportation
Dams	Financial Services	Information Technology	Water and Wastewater Systems



Cybersecurity Risk to Local Governments

- County and municipal cybersecurity
  - Massive organizational risk
  - County and municipal executives often unaware of the risks, wrongfully assuming IT director or CIO has it ‘covered’
- Municipal/County networks contain valuable data to a cybercriminal
  - High value of data AND ease of obtaining



Cybersecurity Risk to Local Governments (continued)

- Local governments are attractive targets because they are connected to state systems or other large networks
- One of the biggest problems facing the public sector is the lack of security professionals

RSA Conference 2017

elliott davis decosimo

- “The myriad smaller governments/entities across the US have major cyber-security problems”
  - Cybersecurity experts panel
- “Challenging to figure out whether there is a single optimal model to govern state cyber-security”
  - Branch Chief for partnerships and engagement at the U.S. Department of Homeland Security
- Data rich environments

RSA Conference 2017 – What’s Next

elliott davis decosimo

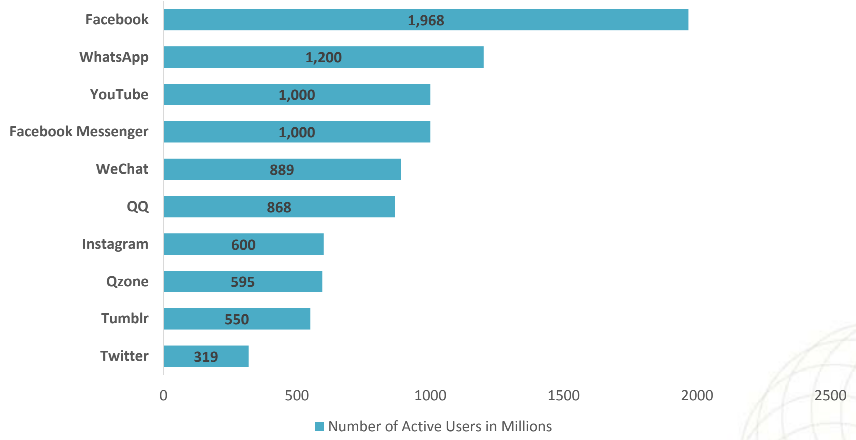
- Prioritize cybersecurity
- Education should be a starting point for most smaller government organizations
- Resource and budget issues
- Elections have elevated the cyber threats and needs

Three core cyber liability risks

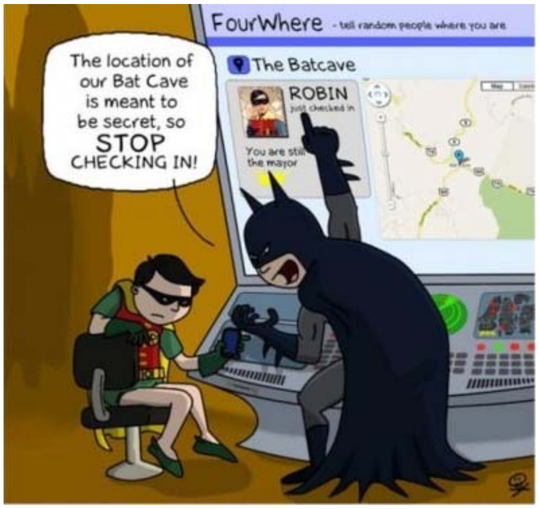
- Technology errors and omissions
  - Network architecture error (i.e. misplaced firewall, unauthorized access), software and hardware do not function properly (i.e. data corruption)
- Social media/e-publishing liability
  - Content ownership (i.e. social media policy), awareness and training
- Data breach of sensitive information
  - HIPAA, negligent/fraud, excessive privilege access, social engineering

Social Networks Scale

- Leading social networks as of April 2017

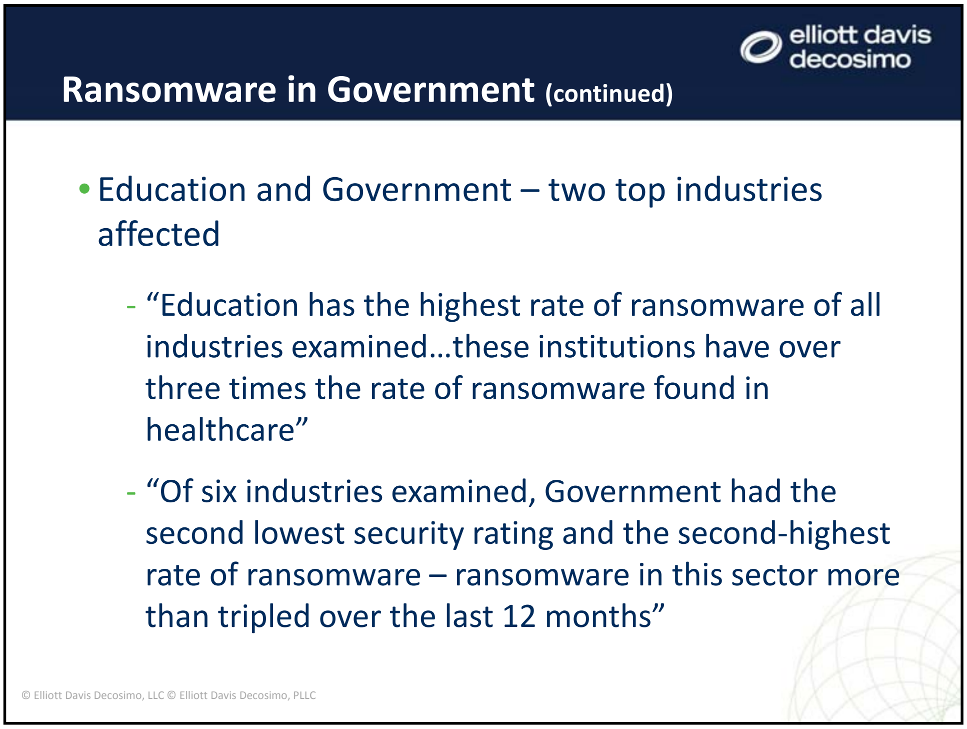


Social Media Cyber Risks


The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!
FourWhere - tell random people where you are
The Batcave
ROBIN just checked in
You are still the mayor

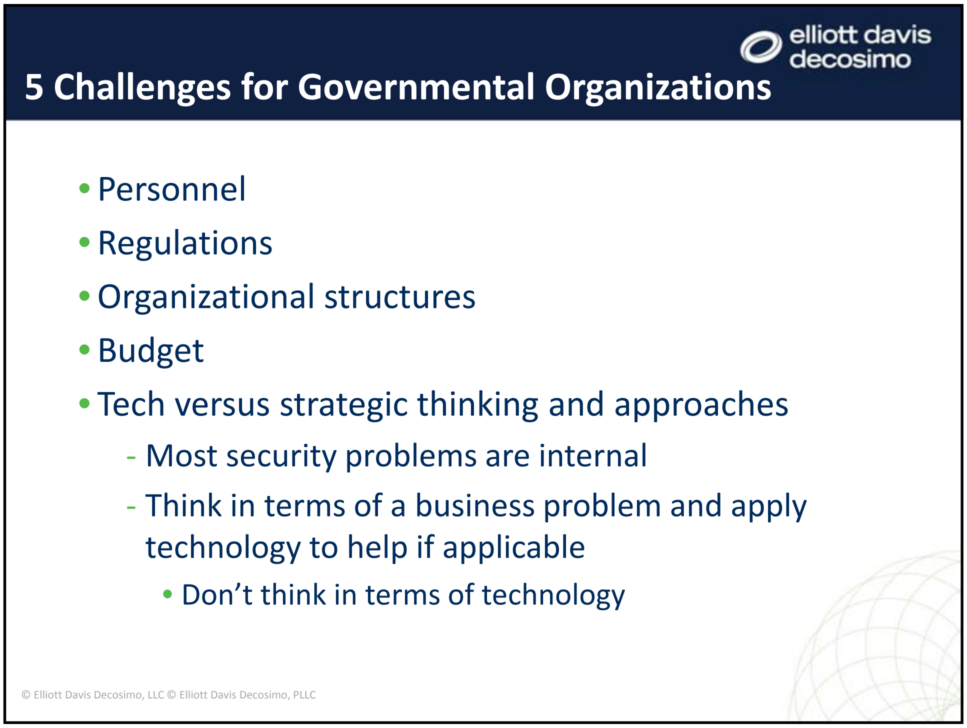
Ransomware in Government

- Phishing attacks with malicious link
- Brute force attack



Ransomware in Government (continued)

- Education and Government – two top industries affected
  - “Education has the highest rate of ransomware of all industries examined…these institutions have over three times the rate of ransomware found in healthcare”
  - “Of six industries examined, Government had the second lowest security rating and the second-highest rate of ransomware – ransomware in this sector more than tripled over the last 12 months”



5 Challenges for Governmental Organizations

- Personnel
- Regulations
- Organizational structures
- Budget
- Tech versus strategic thinking and approaches
  - Most security problems are internal
  - Think in terms of a business problem and apply technology to help if applicable
    - Don’t think in terms of technology

elliott davis decosimo

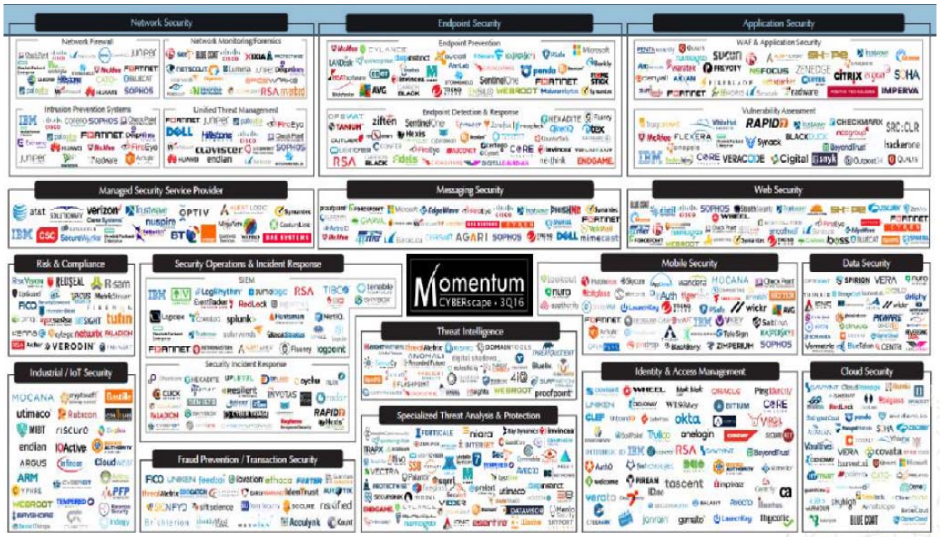
Technical Solution Reliance

Cybersecurity Landscape

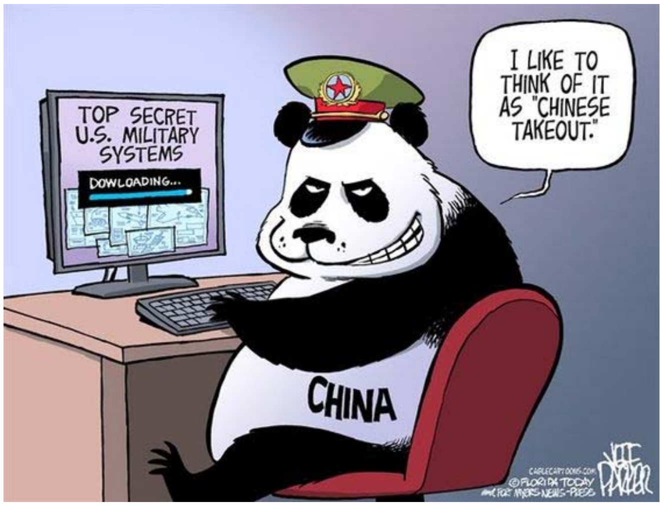
1- Network Security
2- Endpoint Security
3- Web Security
4- Cloud Security
5- Messaging Security
6- Mobile Security
7- Application Security
8- Data Security
9- Managed Security Services
10- Security Operation & Incident Response
11- Threat Intelligence
12- Identity and Access Management
13- Individual/IoT Security
14- Fraud Prevention/Transactional Security
15- Risk and Compliance
16- Specialized Threat Analysis & Protection

elliott davis decosimo

Technical Solution Reliance

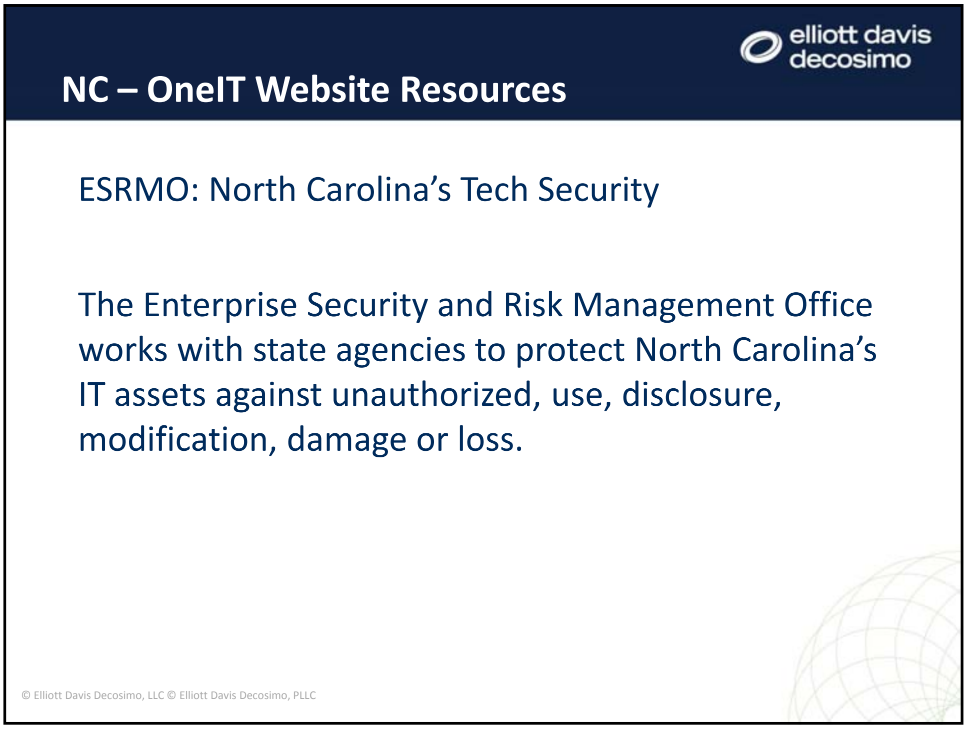

Network Security
Network Firewall
Network Monitoring/Forensics
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Prevention
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Managed Security Service Provider
Messaging Security
Web Security
Risk & Compliance
Security Operations & Incident Response
SIEM
Security Incident Response
Momentum
CYBERscape • 3Q16
Mobile Security
Data Security
Threat Intelligence
Industrial / IoT Security
Identity & Access Management
Cloud Security
Fraud Prevention / Transaction Security
Specialized Threat Analysis & Protection

Resources Available
Agenda Item # 2


TOP SECRET U.S. MILITARY SYSTEMS
DOWLOADING...
I LIKE TO THINK OF IT AS "CHINESE TAKEOUT."
CHINA
CAGLECARTOONS.COM
© FLORIDA TODAY
and FORT MYERS NEWS-PRESS
JEFF PARKER

Resources

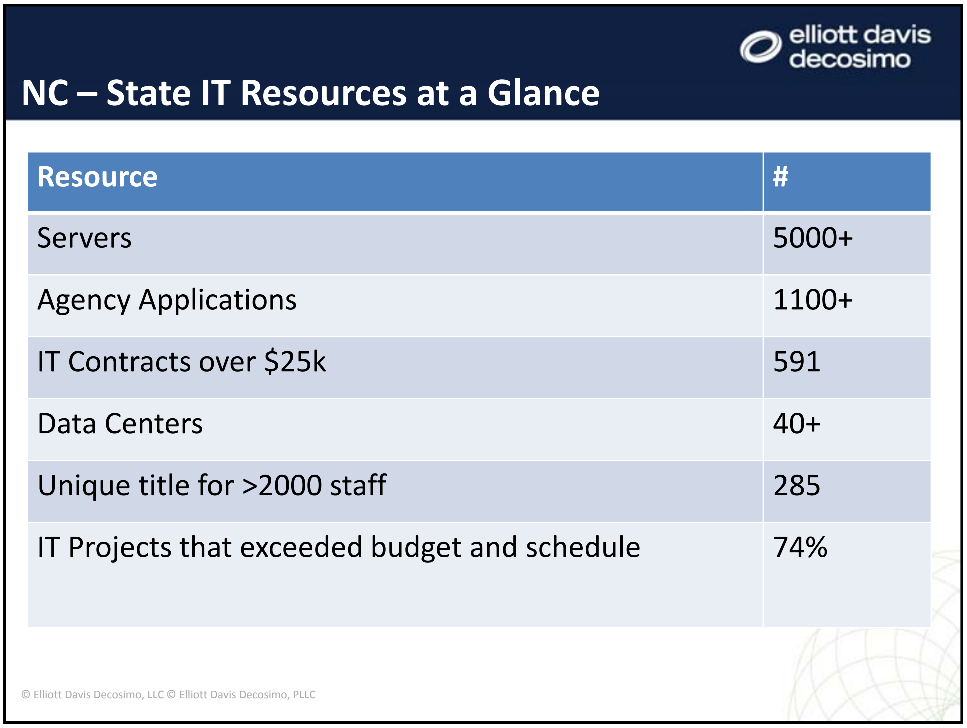
- North Carolina Department of Information Technology
  - OneIT website https://it.nc.gov/oneit
- DHS
  - Grants
- Center for Internet Security (CIS)
  - MS-ISAC
- Various other resources



NC – OneIT Website Resources

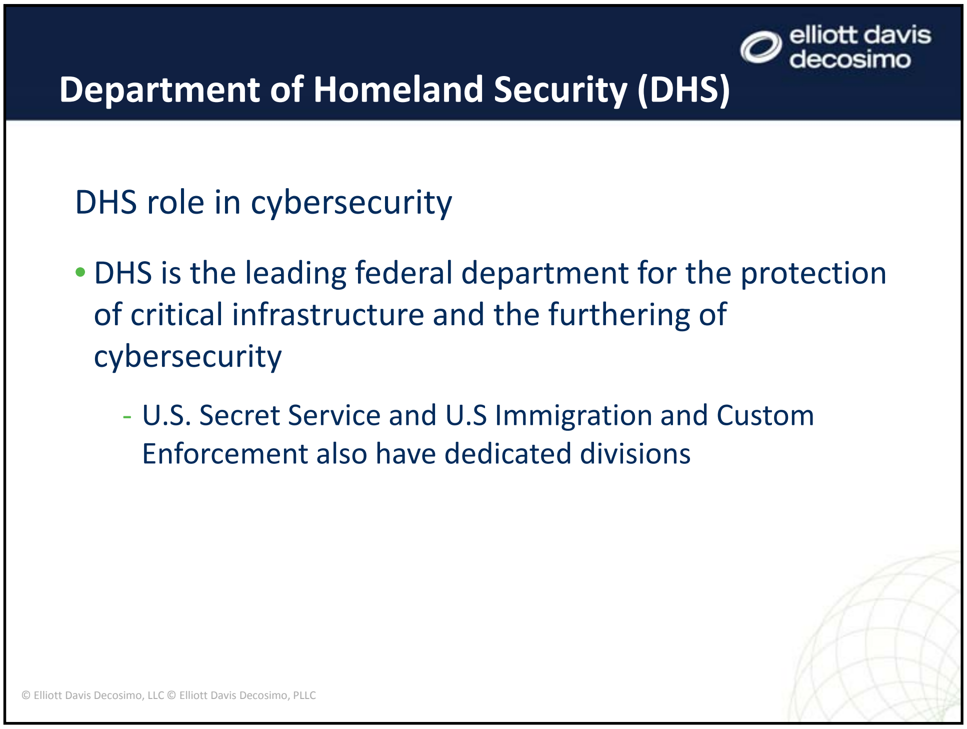
ESRMO: North Carolina’s Tech Security

The Enterprise Security and Risk Management Office works with state agencies to protect North Carolina’s IT assets against unauthorized, use, disclosure, modification, damage or loss.



NC – State IT Resources at a Glance

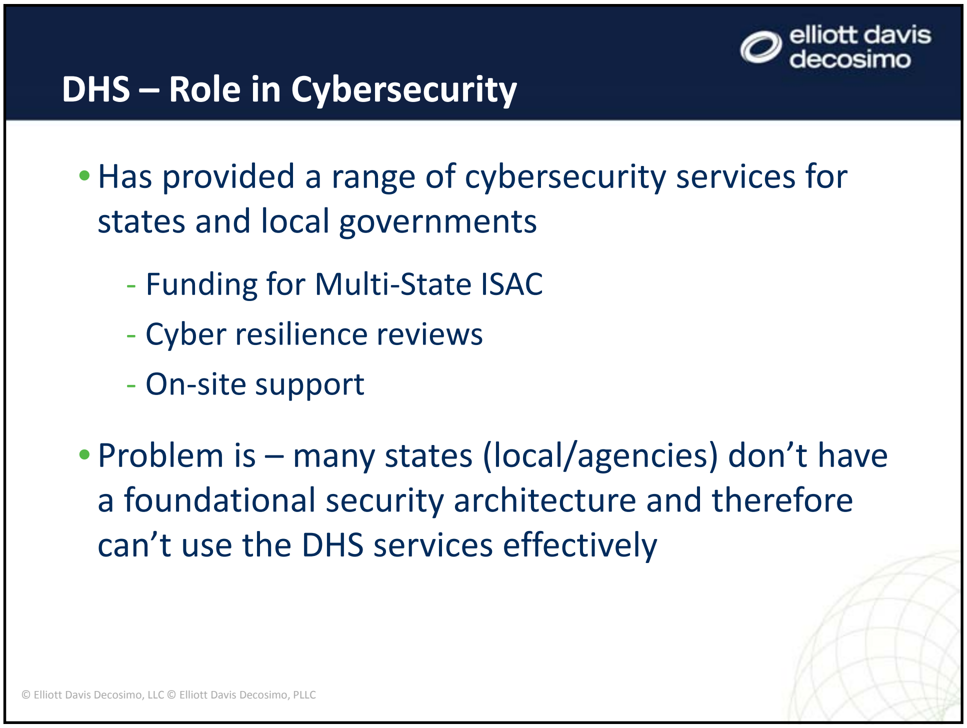
Resource	#
Servers	5000+
Agency Applications	1100+
IT Contracts over $25k	591
Data Centers	40+
Unique title for >2000 staff	285
IT Projects that exceeded budget and schedule	74%



Department of Homeland Security (DHS)

DHS role in cybersecurity

- DHS is the leading federal department for the protection of critical infrastructure and the furthering of cybersecurity
  - U.S. Secret Service and U.S Immigration and Custom Enforcement also have dedicated divisions



DHS – Role in Cybersecurity

- Has provided a range of cybersecurity services for states and local governments
  - Funding for Multi-State ISAC
  - Cyber resilience reviews
  - On-site support
- Problem is – many states (local/agencies) don’t have a foundational security architecture and therefore can’t use the DHS services effectively

elliott davis decosimo

Nationwide Cybersecurity Review - NCSR

- NCSR – Voluntary self-assessment survey
  - Designed to evaluate cybersecurity management
- Who can participate?
  - All States (and agencies), Local governments and departments, Tribal and Territorial governments
- Who are the partners?
  - U.S Department of Homeland Security (DHS)
  - MS-ISAC, a division of CIS, is the focal point for cyber threat prevention, protection, response and recovery

elliott davis decosimo

Center for Internet Security (CIS)

- https://www.cisecurity.org
- Home to Multi-State – Information Sharing and Analysis Center (MS-ISAC)
- Cybersecurity Best Practices
  - CIS Controls
  - CIS Benchmarks
- Cybersecurity Tools
- Cybersecurity Threats

elliott davis decosimo

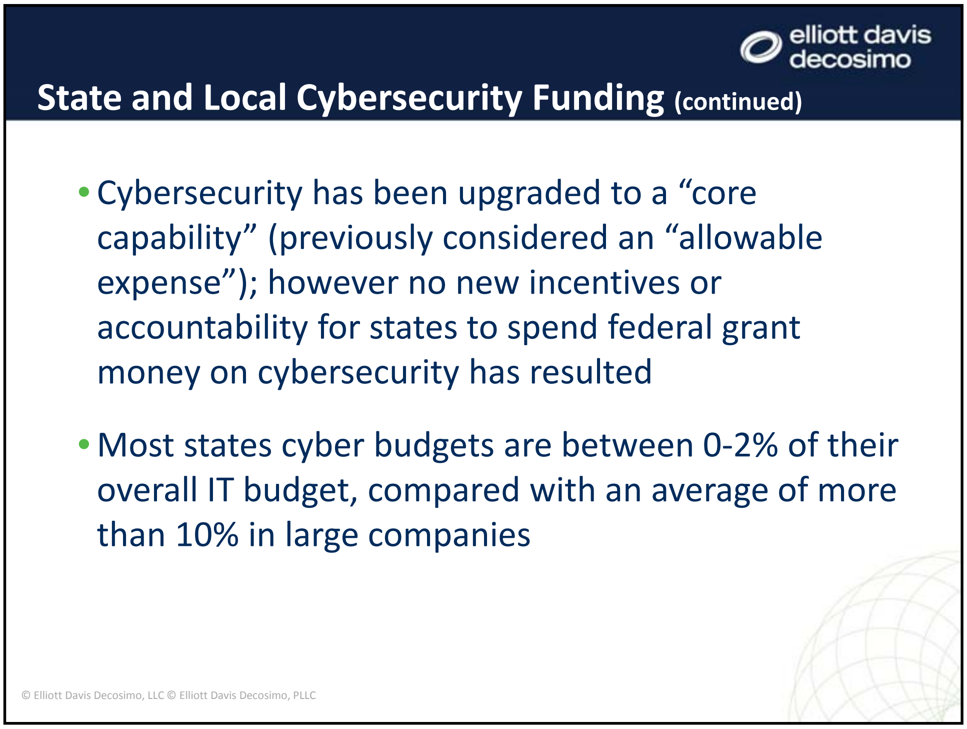
More about MS-ISAC

- Mission
  - To improve the overall cybersecurity posture of state, local, tribal and territorial governments.
  - Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security are the keys to success
- Role
  - MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal and territorial governments
  - 24x7 cybersecurity operations center

elliott davis decosimo

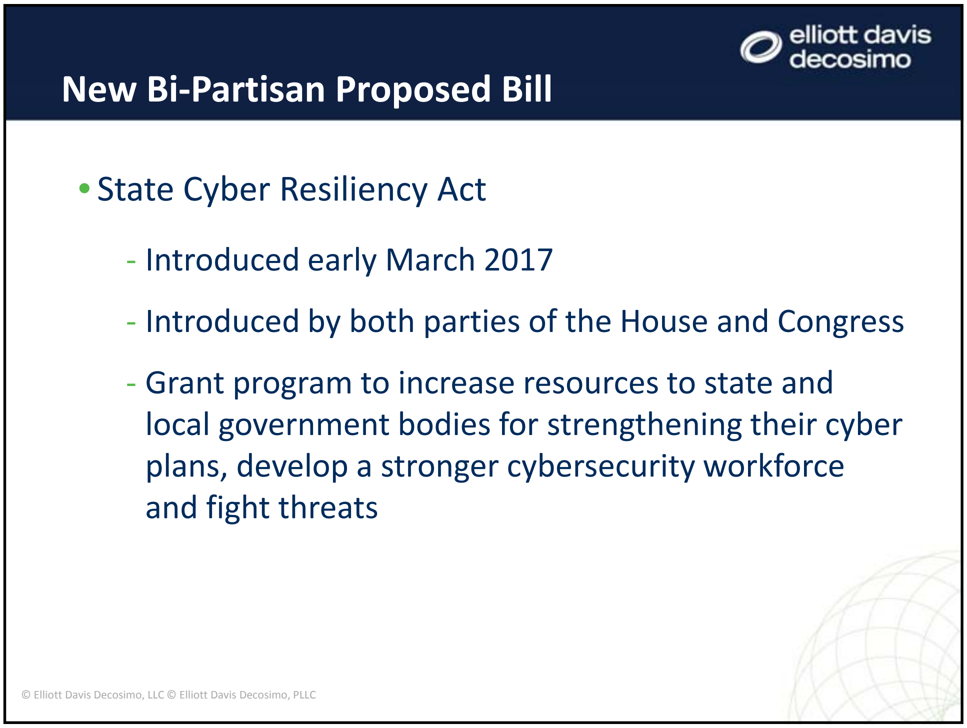
State and Local Cybersecurity Funding

- President’s Commission on enhancing national cybersecurity – released December 2, 2016
  - 70 recommendations, yet one KEY recommendation is missing >> Dire cybersecurity funding needs for state and local governments
  - Department of Homeland Security Grant Program (HSGP) >> $1billion/yr
  - Still, federal cybersecurity funding for states has been overlooked
    - President Obama requested a 37% increase for the 2017 budget



State and Local Cybersecurity Funding (continued)

- Cybersecurity has been upgraded to a “core capability” (previously considered an “allowable expense”); however no new incentives or accountability for states to spend federal grant money on cybersecurity has resulted
- Most states cyber budgets are between 0-2% of their overall IT budget, compared with an average of more than 10% in large companies



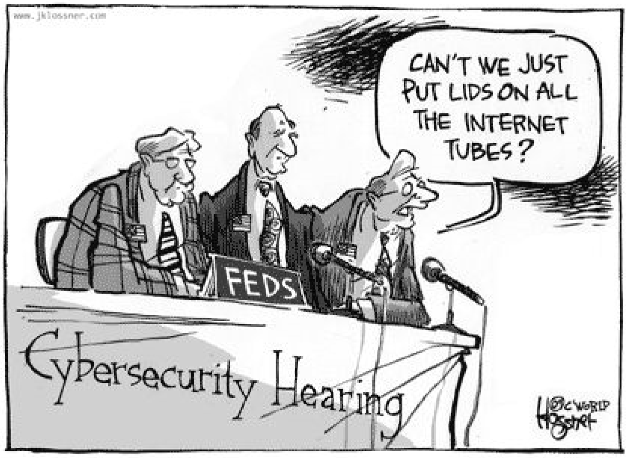
New Bi-Partisan Proposed Bill

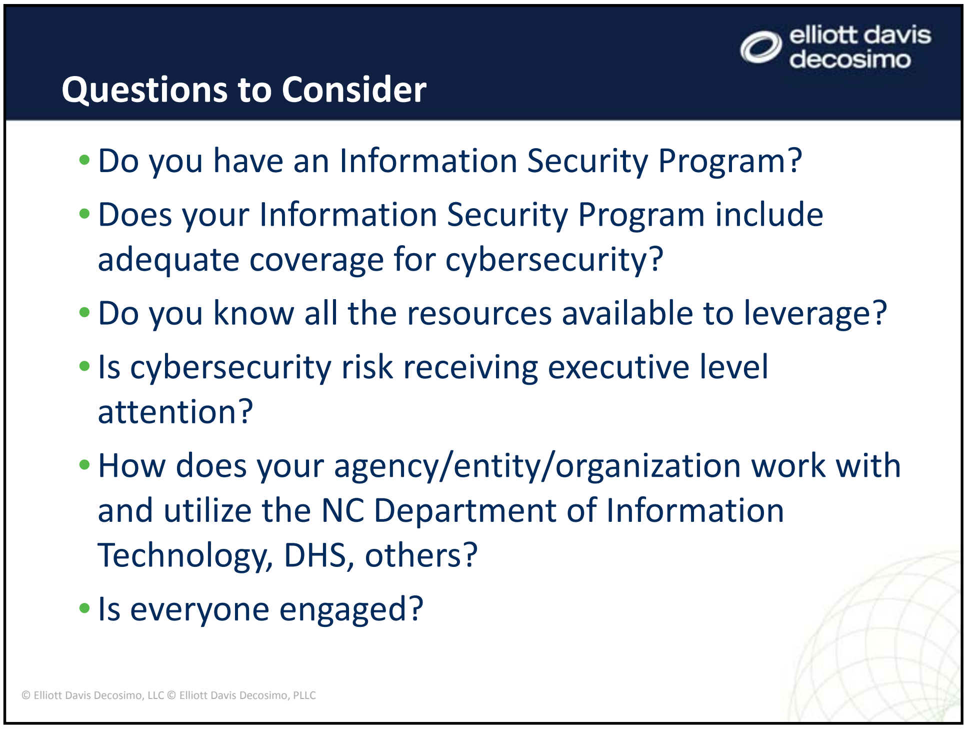
- State Cyber Resiliency Act
  - Introduced early March 2017
  - Introduced by both parties of the House and Congress
  - Grant program to increase resources to state and local government bodies for strengthening their cyber plans, develop a stronger cybersecurity workforce and fight threats

New Bi-Partisan Proposed Bill

- Why
  - Bill sponsors claim less than 2% of IT budgets are dedicated to cybersecurity
  - 2015 report cited 50% of state and local governments had experienced over six breaches the previous two years
  - 2016 had 200,000 personal voter records compromised > prompting the Department of Homeland Security to label the state voting infrastructure as 'critical infrastructure'

Recommendations
Agenda Item # 3

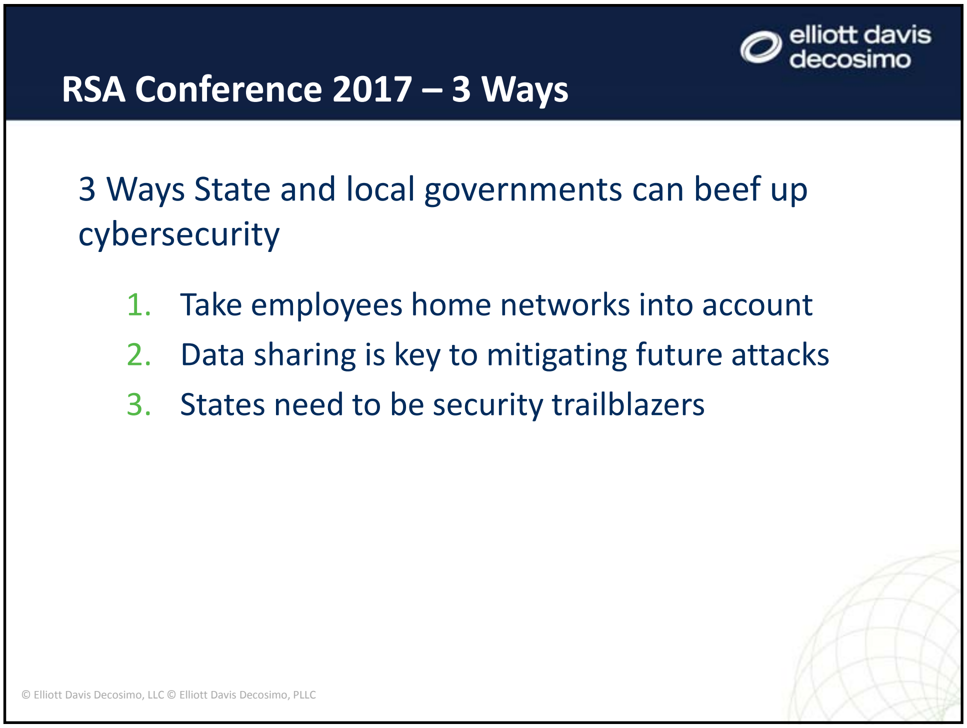




Questions to Consider

elliott davis decosimo

- Do you have an Information Security Program?
- Does your Information Security Program include adequate coverage for cybersecurity?
- Do you know all the resources available to leverage?
- Is cybersecurity risk receiving executive level attention?
- How does your agency/entity/organization work with and utilize the NC Department of Information Technology, DHS, others?
- Is everyone engaged?

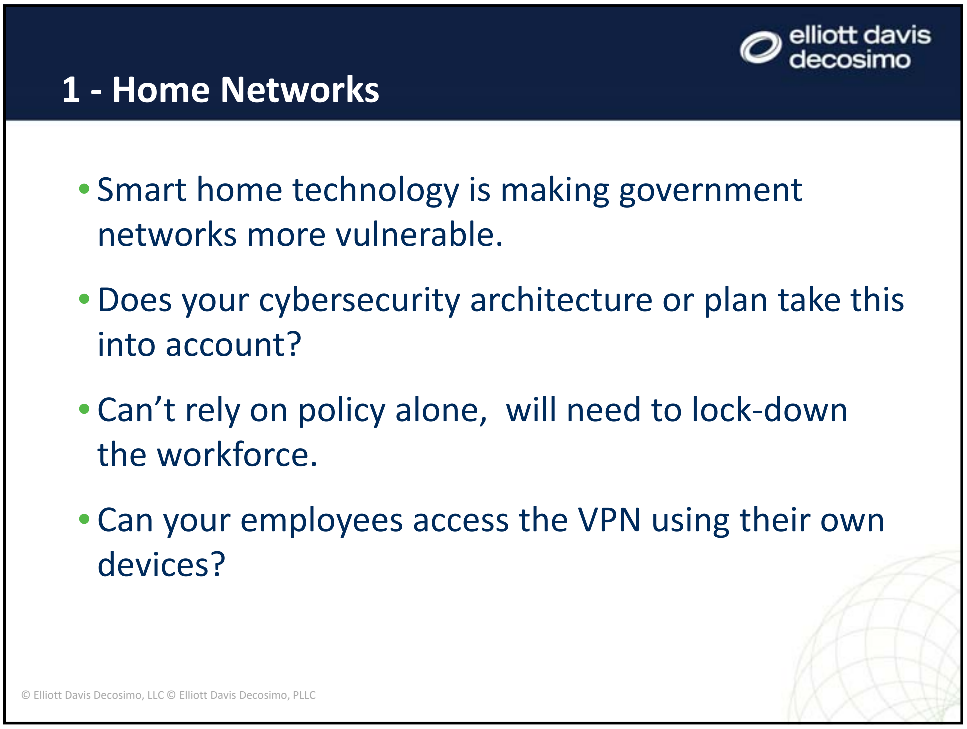


RSA Conference 2017 – 3 Ways

elliott davis decosimo

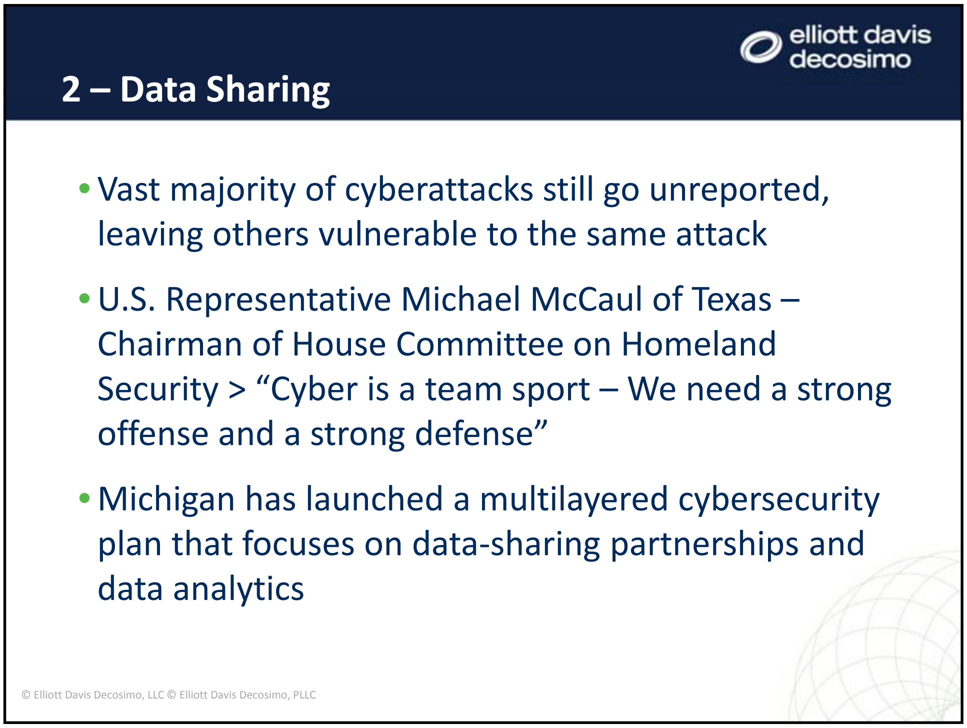
3 Ways State and local governments can beef up cybersecurity

1. Take employees home networks into account
2. Data sharing is key to mitigating future attacks
3. States need to be security trailblazers



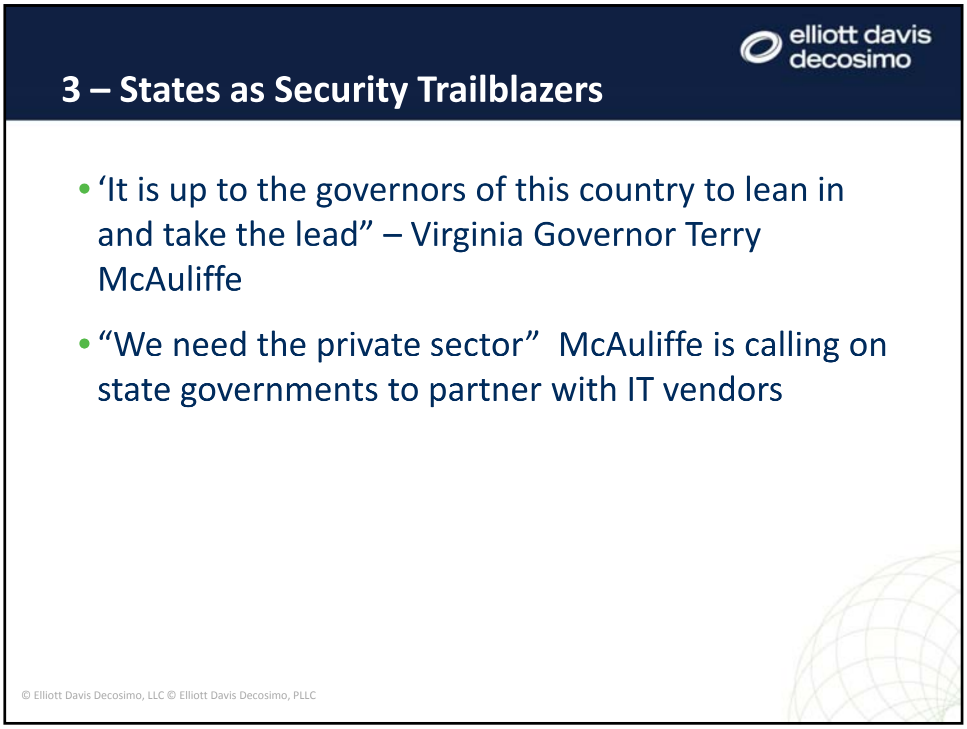
1 - Home Networks

- Smart home technology is making government networks more vulnerable.
- Does your cybersecurity architecture or plan take this into account?
- Can’t rely on policy alone, will need to lock-down the workforce.
- Can your employees access the VPN using their own devices?



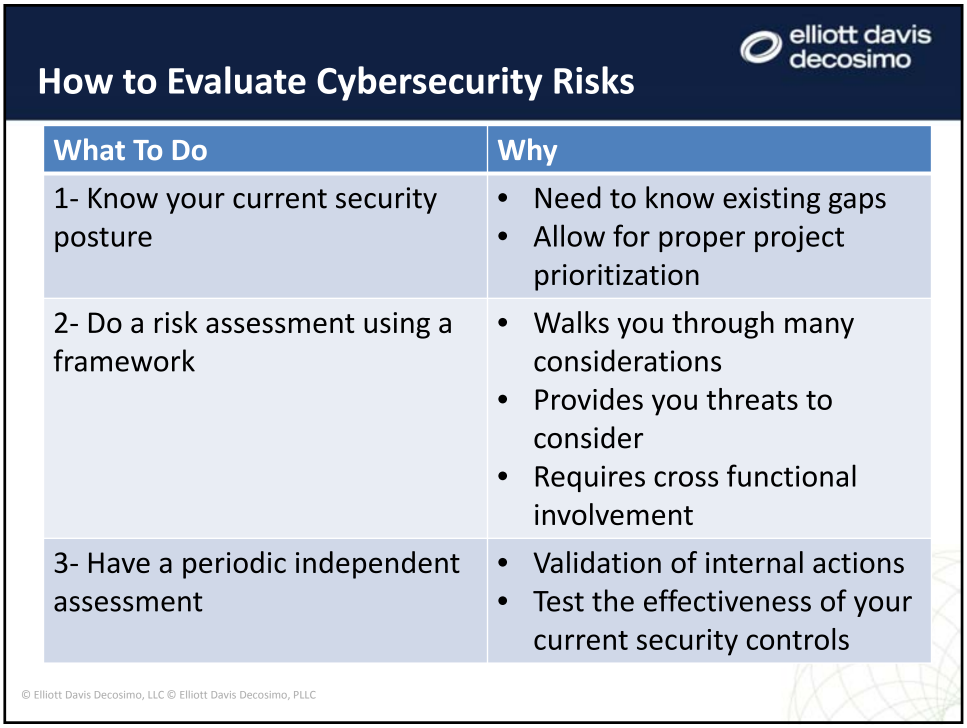
2 – Data Sharing

- Vast majority of cyberattacks still go unreported, leaving others vulnerable to the same attack
- U.S. Representative Michael McCaul of Texas – Chairman of House Committee on Homeland Security > “Cyber is a team sport – We need a strong offense and a strong defense”
- Michigan has launched a multilayered cybersecurity plan that focuses on data-sharing partnerships and data analytics



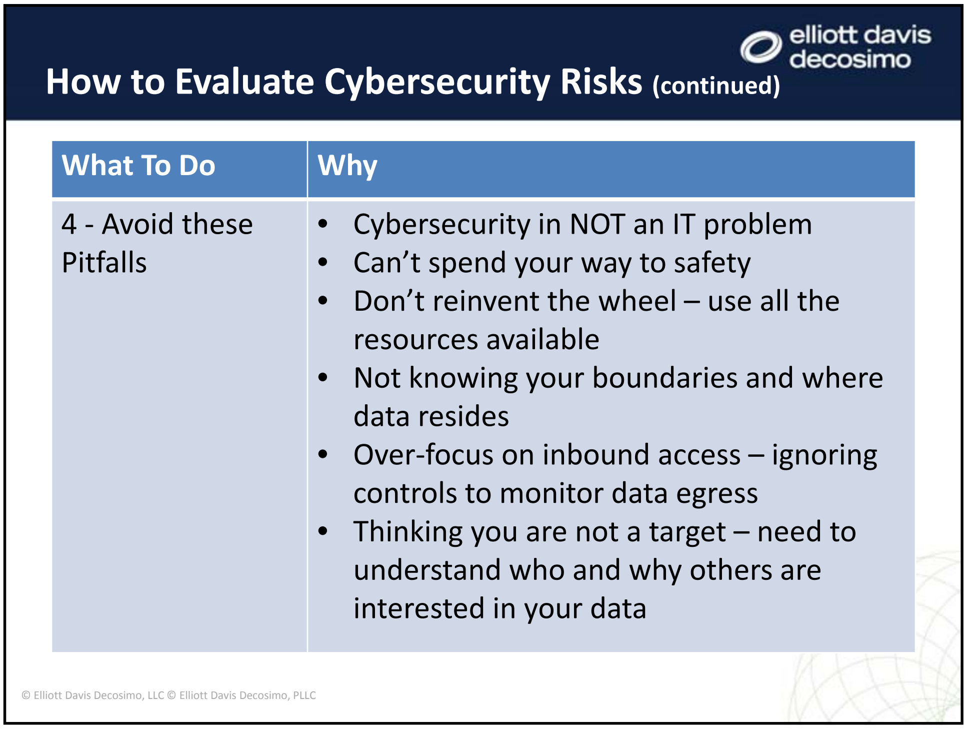
3 – States as Security Trailblazers

- ‘It is up to the governors of this country to lean in and take the lead” – Virginia Governor Terry McAuliffe
- “We need the private sector” McAuliffe is calling on state governments to partner with IT vendors



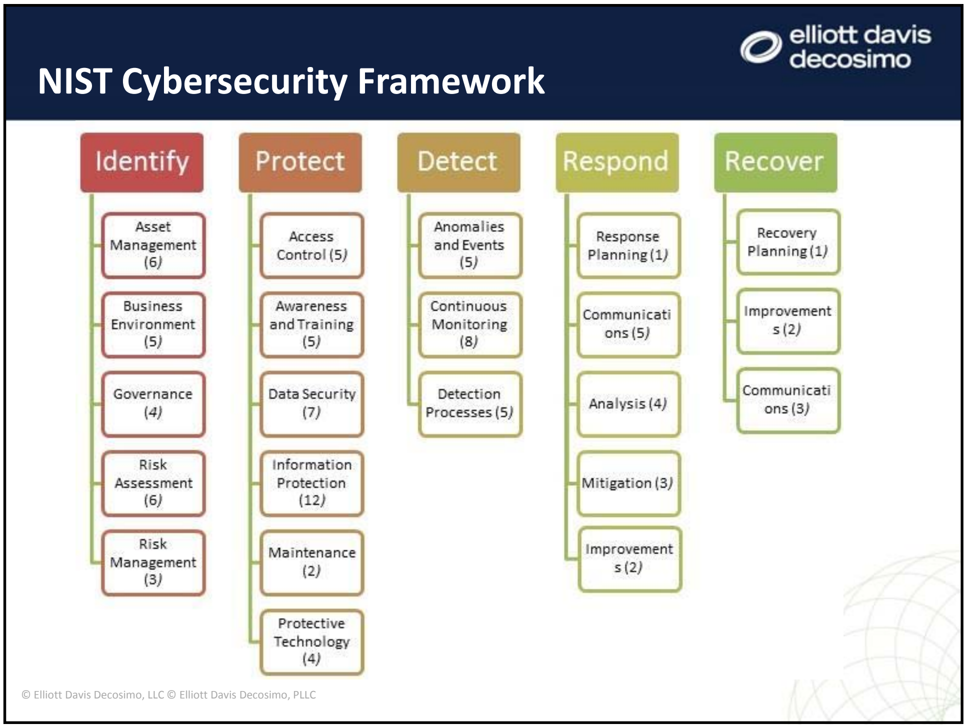
How to Evaluate Cybersecurity Risks

What To Do	Why
1- Know your current security posture	• Need to know existing gaps • Allow for proper project prioritization
2- Do a risk assessment using a framework	• Walks you through many considerations • Provides you threats to consider • Requires cross functional involvement
3- Have a periodic independent assessment	• Validation of internal actions • Test the effectiveness of your current security controls



How to Evaluate Cybersecurity Risks (continued)

What To Do	Why
4 - Avoid these Pitfalls	• Cybersecurity in NOT an IT problem • Can't spend your way to safety • Don't reinvent the wheel – use all the resources available • Not knowing your boundaries and where data resides • Over-focus on inbound access – ignoring controls to monitor data egress • Thinking you are not a target – need to understand who and why others are interested in your data



NIST Cybersecurity Framework

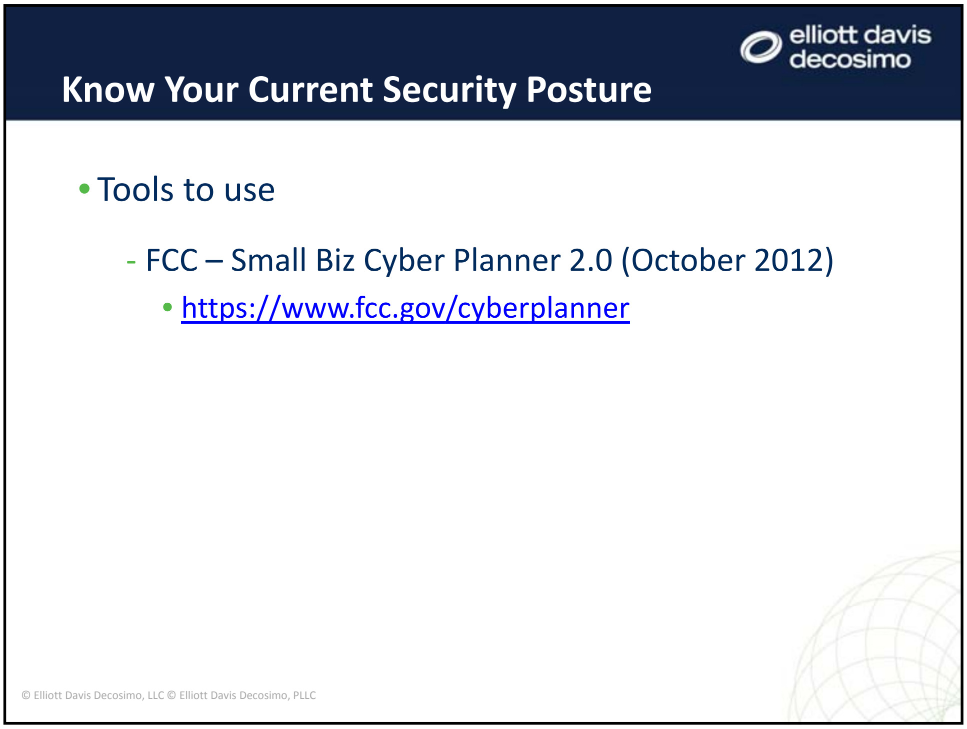
Identify
- Asset Management (6)
- Business Environment (5)
- Governance (4)
- Risk Assessment (6)
- Risk Management (3)

Protect
- Access Control (5)
- Awareness and Training (5)
- Data Security (7)
- Information Protection (12)
- Maintenance (2)
- Protective Technology (4)

Detect
- Anomalies and Events (5)
- Continuous Monitoring (8)
- Detection Processes (5)

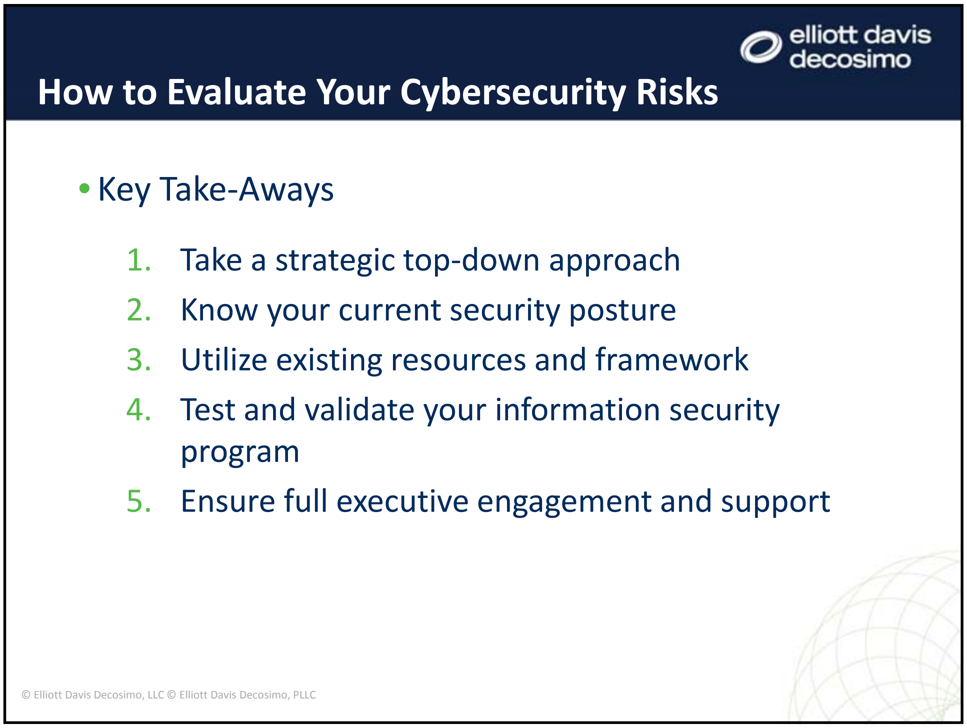
Respond
- Response Planning (1)
- Communications (5)
- Analysis (4)
- Mitigation (3)
- Improvements (2)

Recover
- Recovery Planning (1)
- Improvements (2)
- Communications (3)



Know Your Current Security Posture

- Tools to use
  - FCC – Small Biz Cyber Planner 2.0 (October 2012)
    - https://www.fcc.gov/cyberplanner



How to Evaluate Your Cybersecurity Risks

- Key Take-Aways
  1. Take a strategic top-down approach
  2. Know your current security posture
  3. Utilize existing resources and framework
  4. Test and validate your information security program
  5. Ensure full executive engagement and support

Latest Update on Cybersecurity Risk
Agenda Item # 4

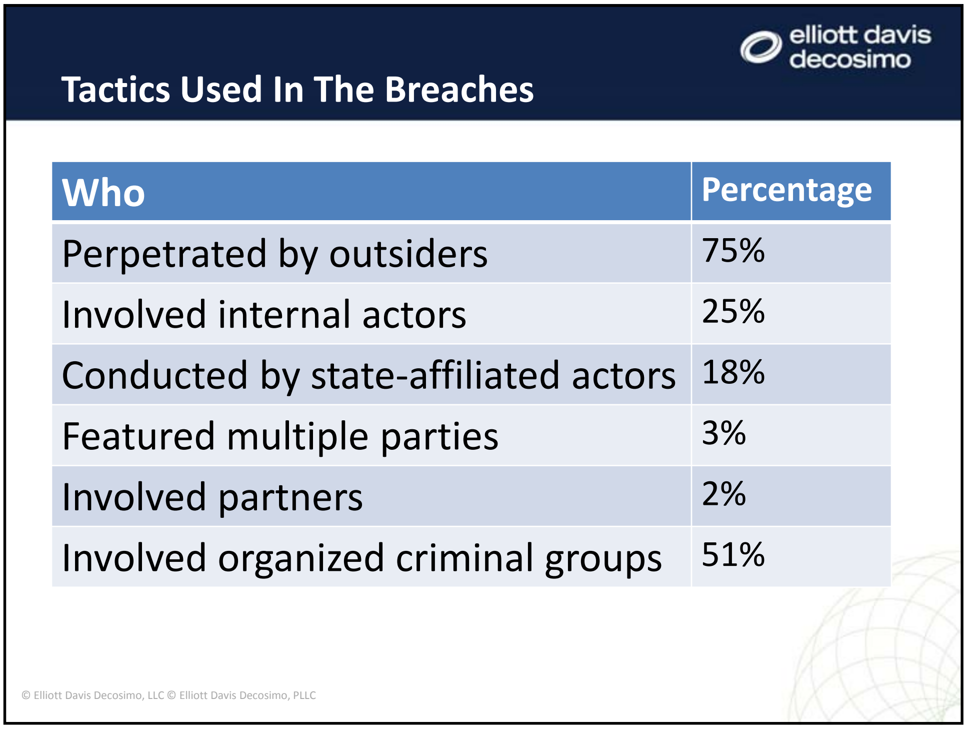
2017 Data Breach Investigations Report
10th Edition
verizon

Ransom Notes are the Most Profitable Form of Writing

Verizon 2017 Data Breach Investigations Report
Contributor

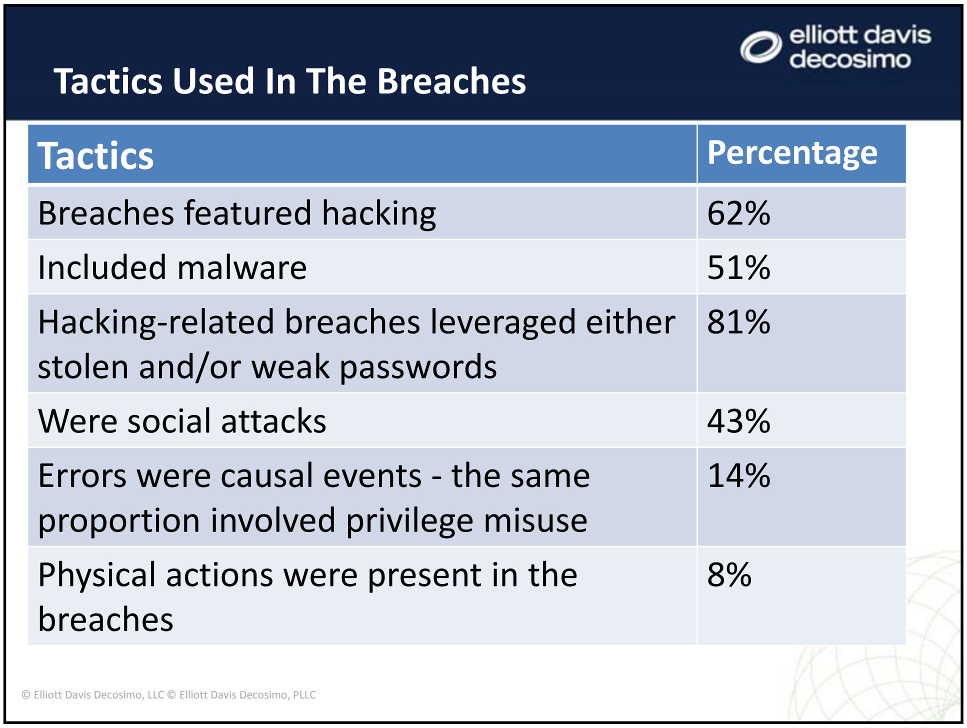
2017 Verizon Data Breach Investigation Report –10th edition

- Incident:
  - A security event that compromises the integrity, confidentiality or availability of an information asset.
- Breach:
  - An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party



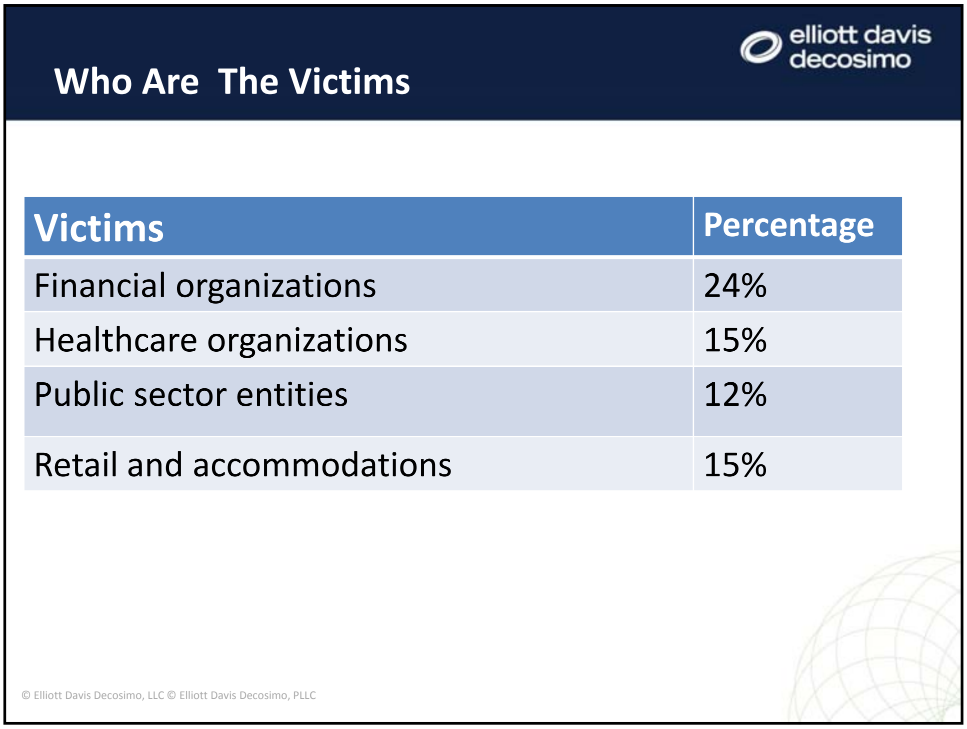
Tactics Used In The Breaches

Who	Percentage
Perpetrated by outsiders	75%
Involved internal actors	25%
Conducted by state-affiliated actors	18%
Featured multiple parties	3%
Involved partners	2%
Involved organized criminal groups	51%



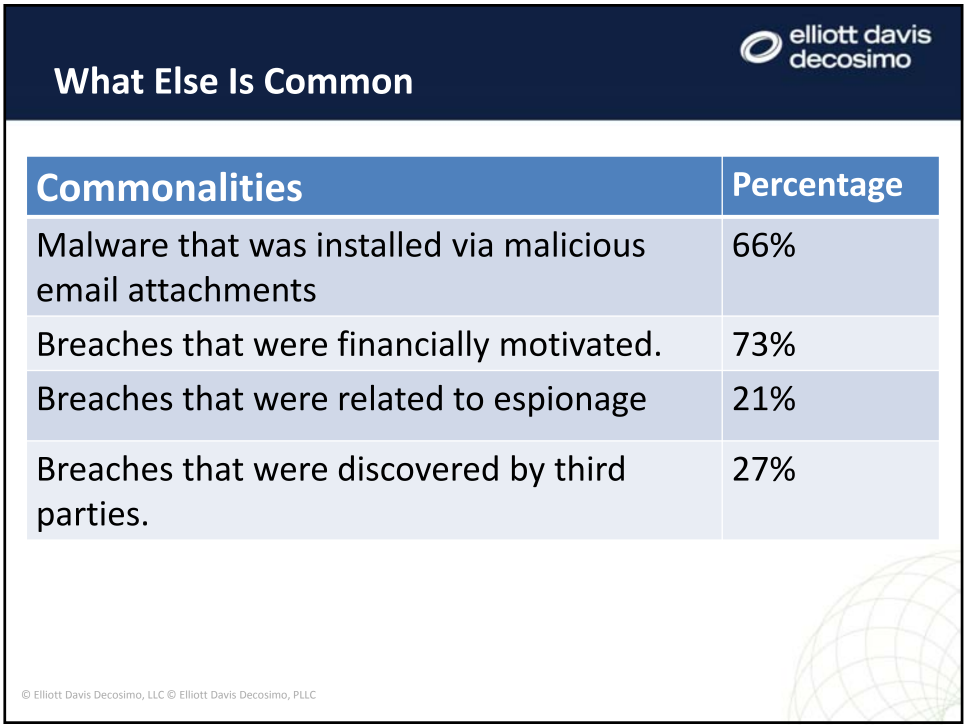
Tactics Used In The Breaches

Tactics	Percentage
Breaches featured hacking	62%
Included malware	51%
Hacking-related breaches leveraged either stolen and/or weak passwords	81%
Were social attacks	43%
Errors were causal events - the same proportion involved privilege misuse	14%
Physical actions were present in the breaches	8%



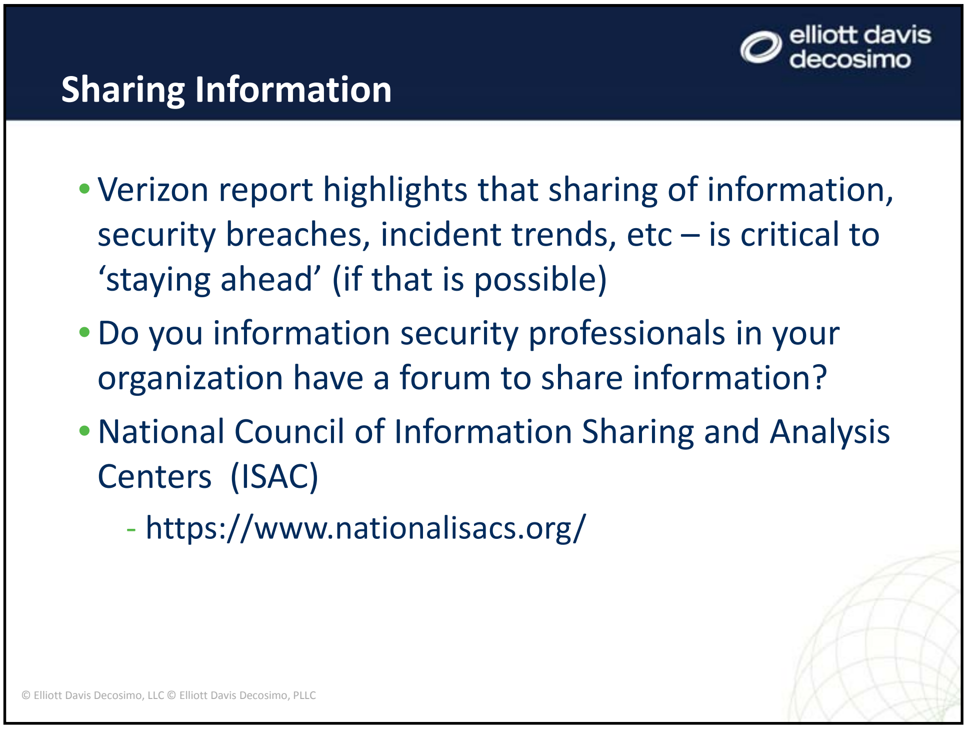
Who Are The Victims

Victims	Percentage
Financial organizations	24%
Healthcare organizations	15%
Public sector entities	12%
Retail and accommodations	15%



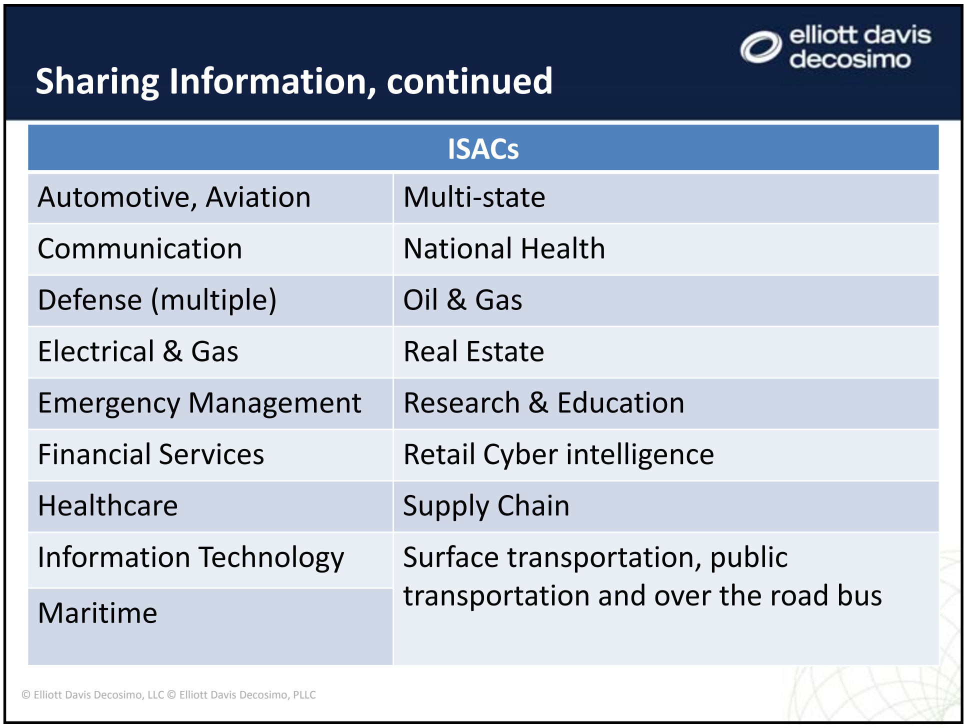
What Else Is Common

Commonalities	Percentage
Malware that was installed via malicious email attachments	66%
Breaches that were financially motivated.	73%
Breaches that were related to espionage	21%
Breaches that were discovered by third parties.	27%



Sharing Information

- Verizon report highlights that sharing of information, security breaches, incident trends, etc – is critical to 'staying ahead' (if that is possible)
- Do you information security professionals in your organization have a forum to share information?
- National Council of Information Sharing and Analysis Centers (ISAC)
  - https://www.nationalisacs.org/



Sharing Information, continued

ISACs	
Automotive, Aviation	Multi-state
Communication	National Health
Defense (multiple)	Oil & Gas
Electrical & Gas	Real Estate
Emergency Management	Research & Education
Financial Services	Retail Cyber intelligence
Healthcare	Supply Chain
Information Technology	Surface transportation, public transportation and over the road bus
Maritime	

Questions

Bonnie Bastow, Director

Email: bonnie.bastow@elliottdavis.com

704.808.5275

Fellen Yang, Manager

Email: fellen.yang@elliottdavis.com

704.808.5290

Website: www.elliottdavis.com

Elliott Davis Decosimo provides comprehensive assurance, tax and consulting solutions to diverse businesses, organizations and individuals. With a network of forward-thinking professionals in major U.S. markets and alliance resources across the globe, the firm ranks among the top 30 and fastest-growing accounting firms in the U.S. Visit elliottdavis.com for more information.