GENEDGE

Cyber (In)Security, The Internet of Things, and Risk Management

Presented by:

Roy Luebke – Innovation and Growth Consultant

October 27, 2016

What is GENEDGE?

MEP • MANUFACTURING EXTENSION PARTNERSHIP
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

GENEDGE

We are the Manufacturing Extension Program of Virginia

A unit of the Commonwealth of Virginia

Part of the Department of Commerce / NIST network of Centers across the country (60 centers, 1500 staff nationally)

20 years of success supporting Virginia businesses

Since 2000, the #1 Bottom-Line and Top-Line Impact Producer in the system – over $3.5 Billion of business impact reported

Over 10,500 industrial jobs created / retained

32 staff including two sub-recipient partners, The Manufacturing Technology Center in SW VA and Old Dominion University in Hampton Roads

What Does GENEDGE Do?

Strategic Innovation and Growth

Continuous Process Improvement

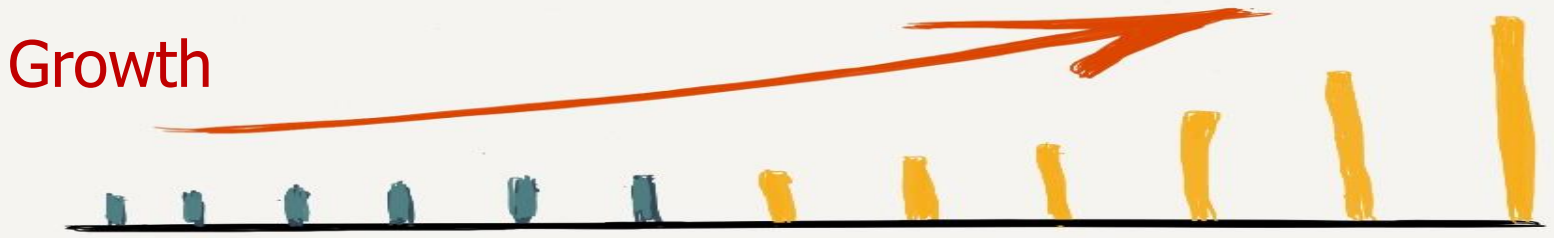
Sustainability

Supply Chain Optimization

Technology Acceleration

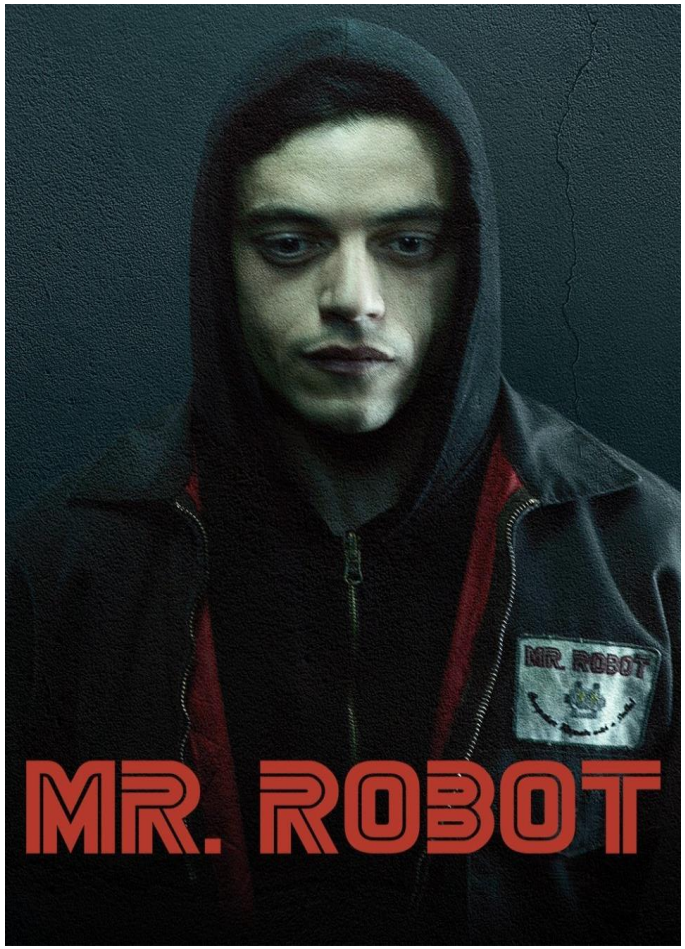
Export Assistance

Market Commercialization



First Thing To Know…..

YOU HAVE ALREADY BEEN COMPROMISED



First Thing To Know…..

There is no such thing as cyber <u>security</u>

…… only more secure or less secure

…… the degree is a matter of money and priorities

Symantec 2016 Security Report (for 2015)

A New Zero-Day Vulnerability Discovered Each Week

Half a Billion Personal Records Stolen or Lost

Spear-Phishing Campaigns Targeting Employees Increased 55 Percent

Ransomware Increased 35 Percent

100 Million Fake Technical Support Scams Blocked

430 million new unique pieces of malware in 2015, up 36 percent from the year before

Major Security Vulnerabilities in Three Quarters of Popular Websites Put Us All at Risk

New Mobile vulnerabilities increased 214%

What's Happening in Cyber

- Indiscriminate Attacks
- Destructive Attacks
- Cyber Warfare
- Espionage: Both Corporate and Government
- Email and login
- Financial and personal information
- Medical information
- Hackivism

Types of Cyber Issues - Technical

- *Vulnerability of a system*

  Eavesdropping
  Spyware
  Phishing
  Espionage

- *Exploits to/within a system*

  Trojans
  Virus and worms
  Denial of service
  Botnets
  Adware
  Dialers
  Ransomware

- *Payloads delivered onto a system*

  Rootkits
  Keyloggers

Serious Bad Guys

China
PLA Unit 61398

Military Unit Cover Designator (MUCD) of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks.

Russia
FSB/KGB

the Russian signals intelligence, which is currently a part of the FSB but has been formerly a part of 16th KGB department, but others are directed by the Russian Ministry of Internal Affairs and the Military of Russia.

What Is Cyber "Security"?

Prevention --- Where the $ have been in past

Detection ---- Where the $ are moving to now

Responses ---- Taking action during the attack

Recovery ---- Fixing the damages of an attack

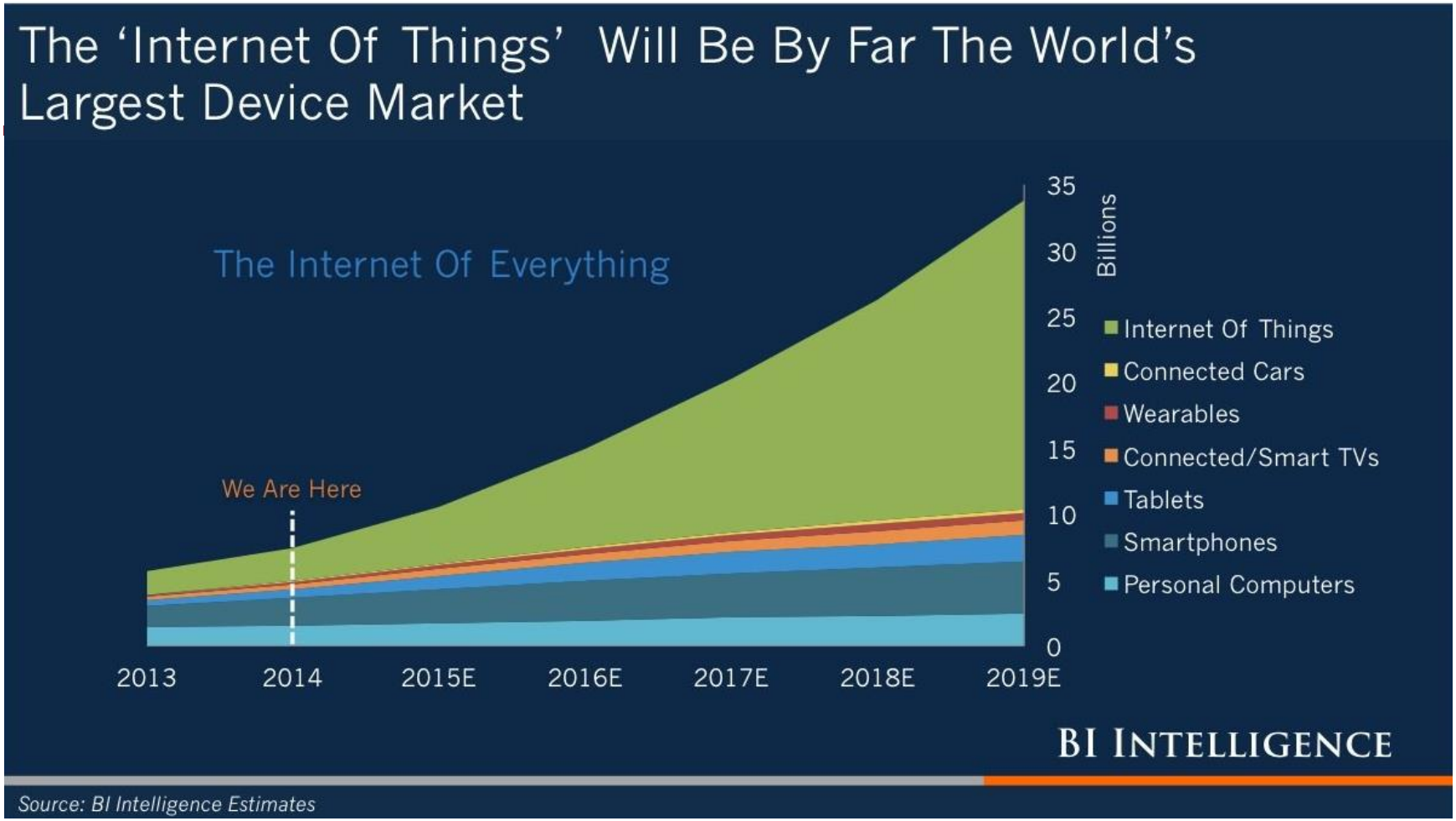
What Is Coming in Cyber Next?

Internet of Things:

- Cars
- Smart home devices
- Medical devices
- Smart TV's
- Embedded devices

Gartner: 6 billion things connected by 2016

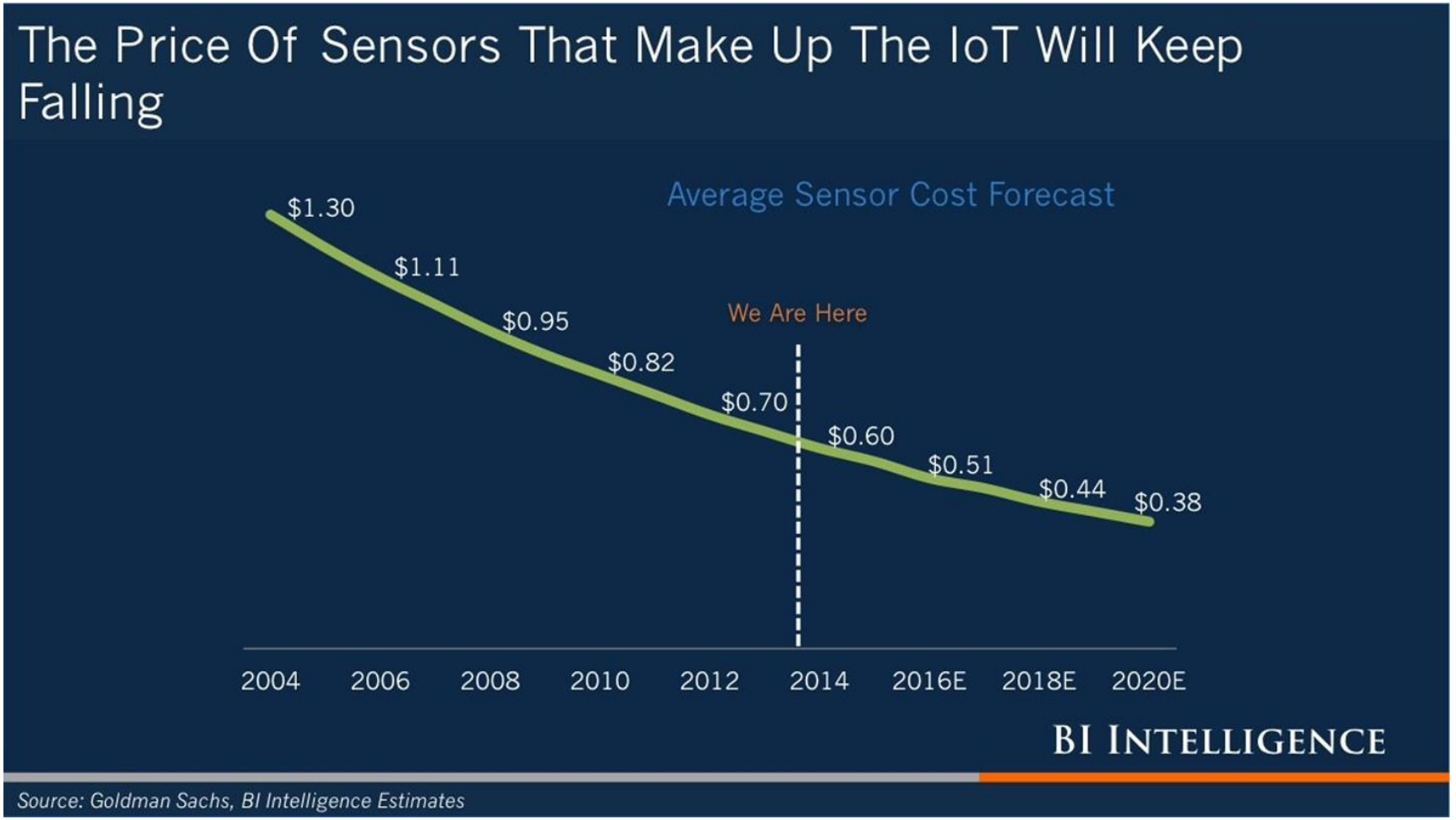
21 billion things by 2020



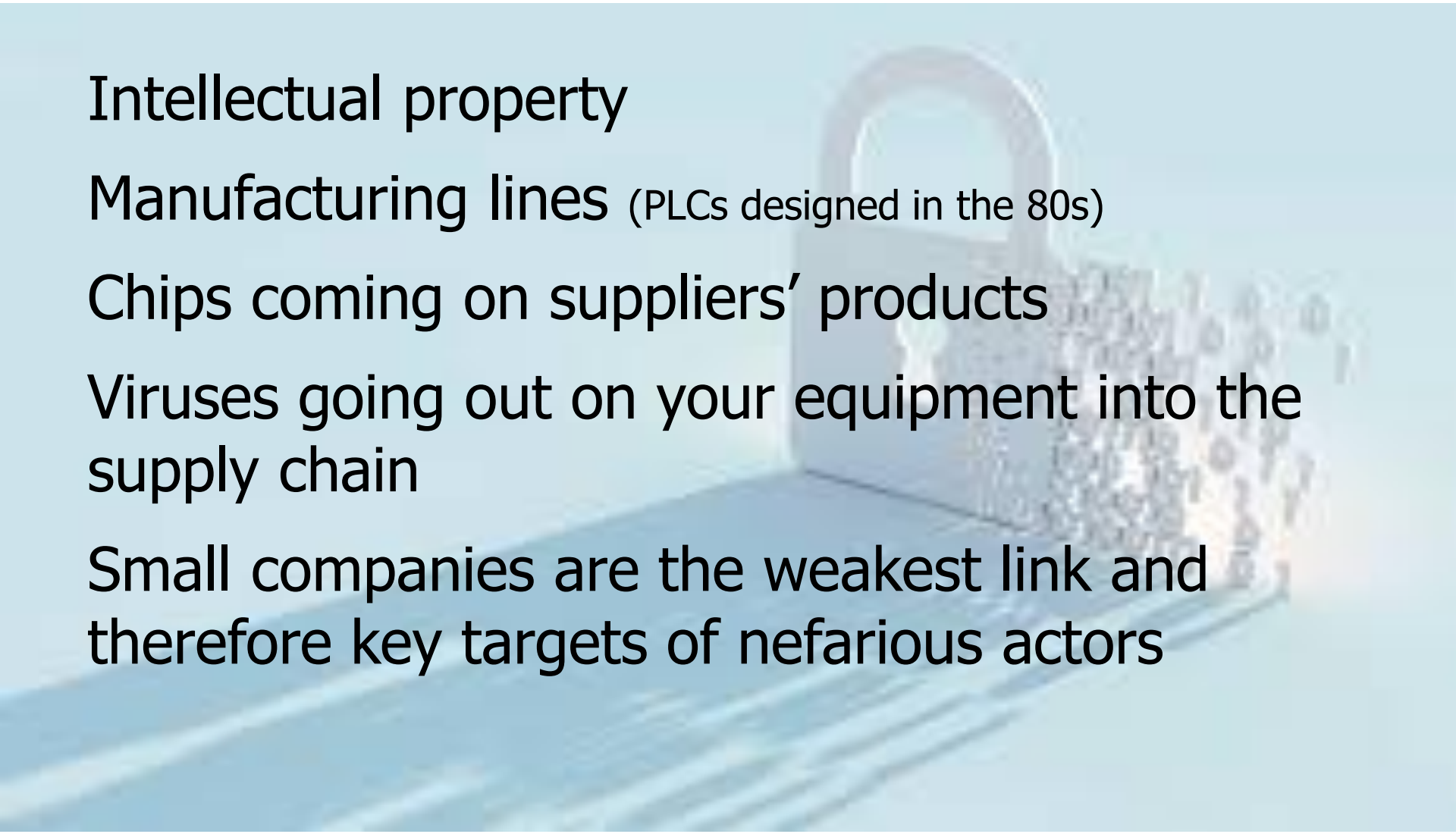
IoT will cause IP traffic to reach 1.6 zettabytes by 2018, a 300% rise on 2013's figures.

Is the IoT Really ‘Internet of Sensors’?

May 8, 2015 by George Leopold in *Enterprise Tech*



Manufacturing Threats



- Intellectual property
- Manufacturing lines (PLCs designed in the 80s)
- Chips coming on suppliers' products
- Viruses going out on your equipment into the supply chain
- Small companies are the weakest link and therefore key targets of nefarious actors

What Happens When You're Hit?

Most Small Businesses Don't Recover

- 20% of all cyber-attacks hit small businesses with 250 or fewer employees
- Nearly 60% of small businesses go out of business within 6 months after being victimized by cybercrime.

http://smallbusiness.foxbusiness.com/technology-web/2013/03/21/most-small-businesses-dont-recover-from-cybercrime/

Small businesses face greater threat from computer hackers

October 12, 2015:

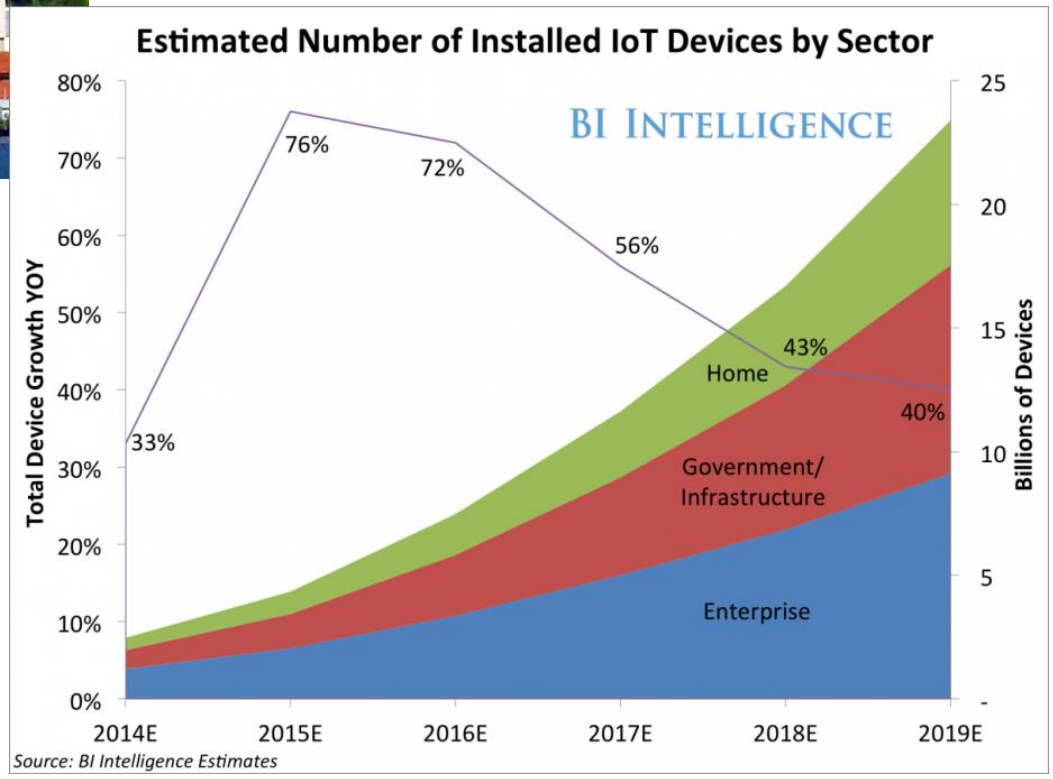
- Small businesses are increasingly being targeted because their security is not as tough.
- 60 per cent of businesses hit by a cyber attack went out of business within six months.

http://threatbrief.com/small-businesses-face-greater-threat-from-computer-hackers-report-warns/

The Industrial Internet

How Many?

- Transportation
- Utility
- Communications
- Business/IT
- Military/LE
- Consumer



The Internet of Industrial Things

http://bits.blogs.nytimes.com/2015/10/14/g-e-navigates-carefully-the-industrial-internet-of-things/?_r=2&mtrref=undefined

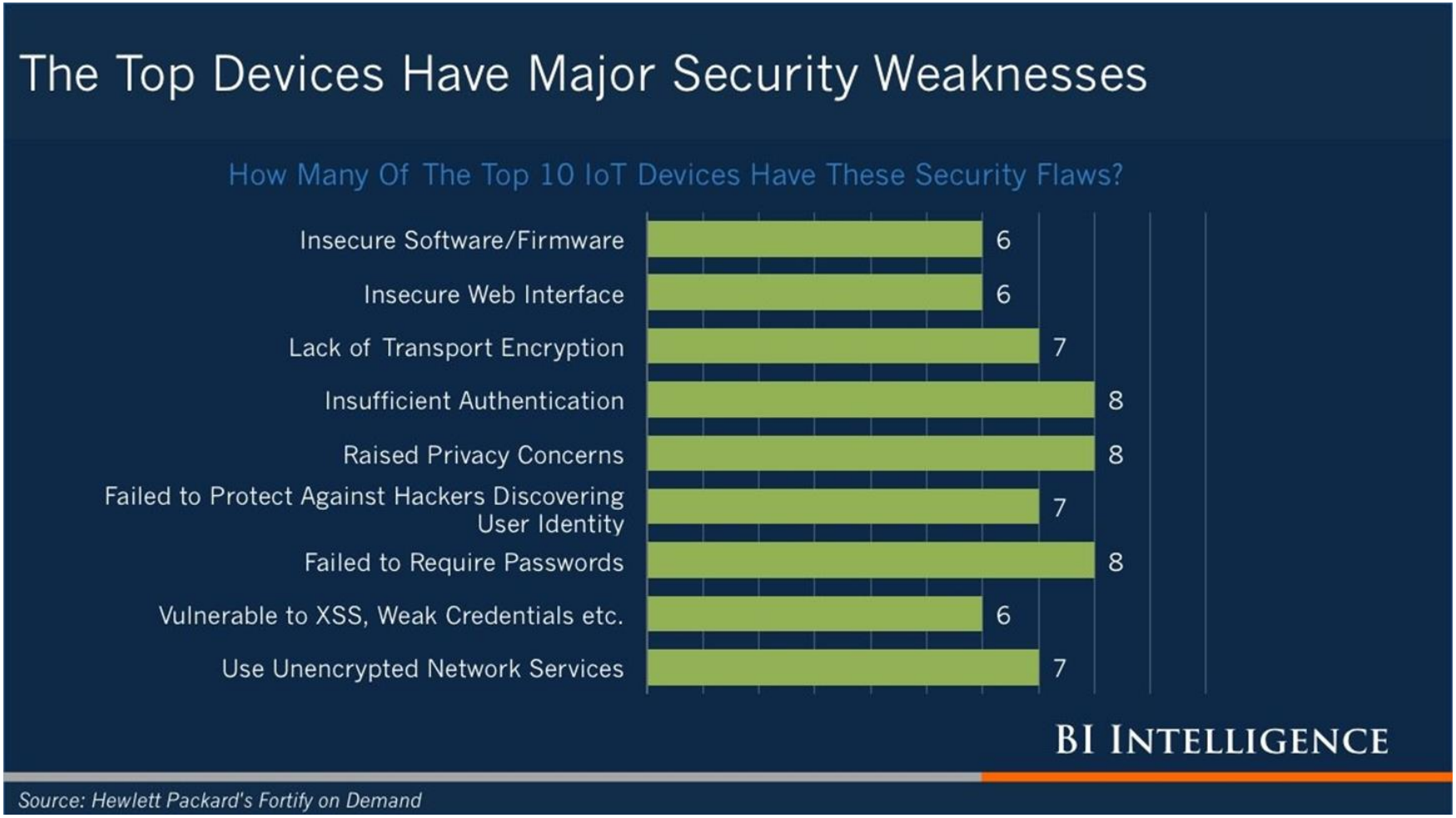
Gas turbines made at a General Electric plant in South Carolina are equipped with more than 3,000 sensors.Credit Mike Belleme for The New York Times

The market for industrial digital security products and services is more than $2 billion a year and increasing 15% annually

Sid Snitkin of ARC Advisory Group, a research firm.

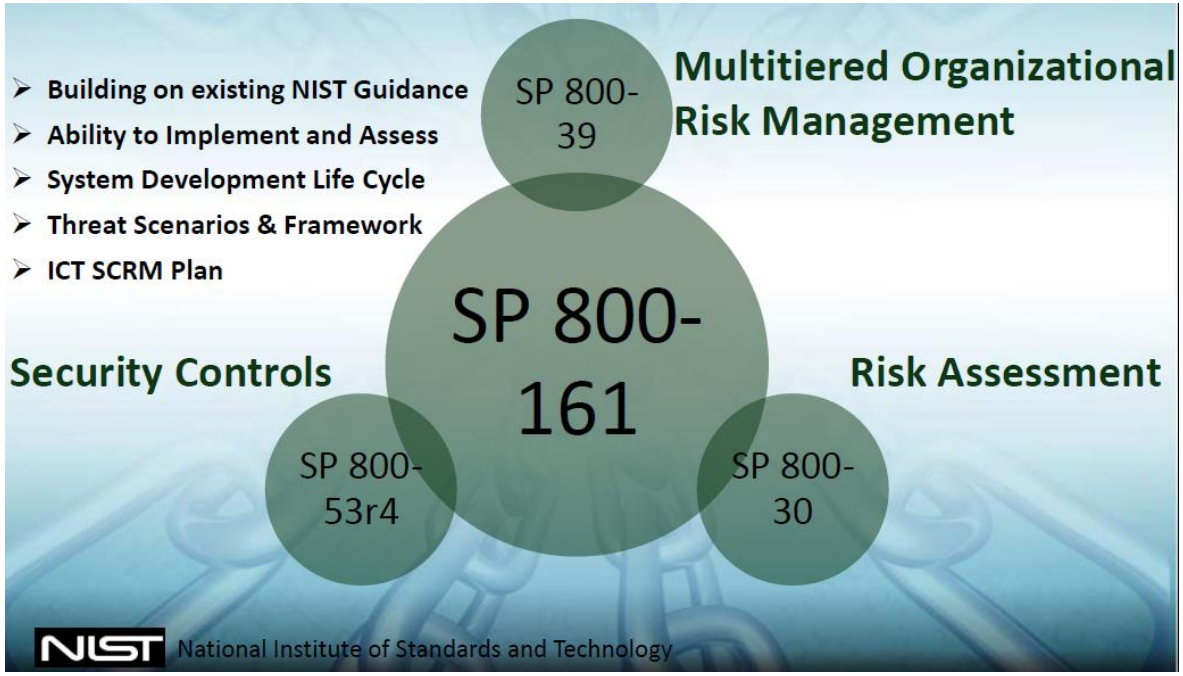
G.E. says it monitors the data flowing from 10 million sensors on $1 trillion worth of equipment every day.

Surely It's Fixed…?



Compliance and Liability Requirements Increasing

Courtesy of/Adapted from Joe Jarzombek, Dir. For Software and Supply Chain Assurance, DHS CS&C



If your product contains software, even from a third party, you may be increasingly liable and your product may be considered defective, unless you:

- **Avoid accepting software with *malware* pre-installed**
- **Determine that no publicly reported *vulnerabilities* remain in code**
- **Determine that exploitable software *weaknesses* are mitigated**

…prior to operational acceptance

More Money Spent on Regulations

U.S. Mid-Atlantic manufacturers on average have devoted more money to complying with regulations than to security on either their data and networks, or equipment and workers, a Philadelphia Federal Reserve 2016 survey showed.

FEDERAL RESERVE BANK OF PHILADELPHIA

NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- Prime contractors AND
- Subcontractors

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

DFARS for Defense Contractors

- Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI)

- Safeguarding covered defense information and cyber incident reporting

- Must be compliant by 12/31/2017

For Small Business CEOs

Virus protection

Firewall

Email filter

IS NOT GOING TO PROTECT YOUR ASSETS

Who's Problem Is It?

It is not an IT problem…..

It is a **LEADERSHIP** *risk management* issue

What Is The Solution?

You Are Already Compromised!

Your systems and infrastructure are already breached, you just have not found out yet.

Significant risk exposure to loss of intellectual property, customer and staff information, and connections to partners through breaches to IT infrastructure, communications, and automated systems.

Risk exposure in manufacturing production by having cyber threats unintentionally installed on products via chips, or any internet connectivity to or through products.

Loss of IT infrastructure, or having cyber threats placed onto their offerings, could put many firms completely out of business.

Small Businesses Are Targets

Travelers Insurance reports that **62%** of cyber breach victims **are small to medium businesse**s.

Healthcare and Financial are most-breached industries currently

http://www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber

Cyber Breach Cost Components

Business income loss

Defense and settlement costs

Lost customers and damaged reputation

Cyber extortion payments

Forensics costs to discover cause

Regulatory fines

Cost to notify regulators

Cost to notify affected individuals and companies

Cost to rebuild infrastructure, data, etc.

Loss of intellectual property

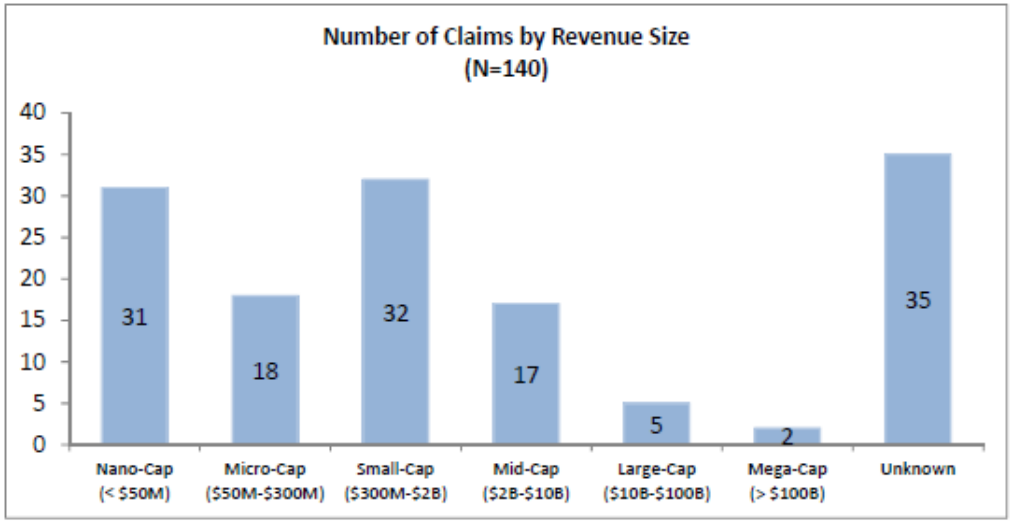
Loss of other assets

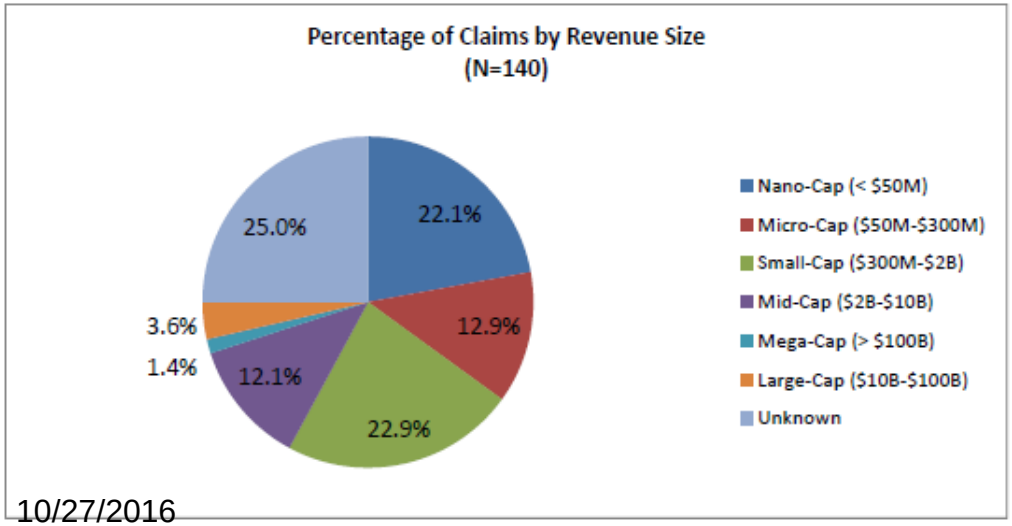
Example Cyber Losses

$30M retailer	$2.5M to $6M
$100M hospital	$380K to $2M
$350M bank	$800K to $1.6M
400 employee manufacturer	$1.7M

http://www.propertycasualty360.com/2015/10/16/hacked-the-cost-of-a-cyber-breach-in-5-different-i

Cyber Insurance





- Risk management mechanism
- Costs of response/recovery
- Awareness to make claim

<u>Policy Payout Data</u>

Avg Nano-cap: $56,000

Avg Micro-cap: $150,000

What is Risk?

The probability and impact of a negative outcome in a given period of time

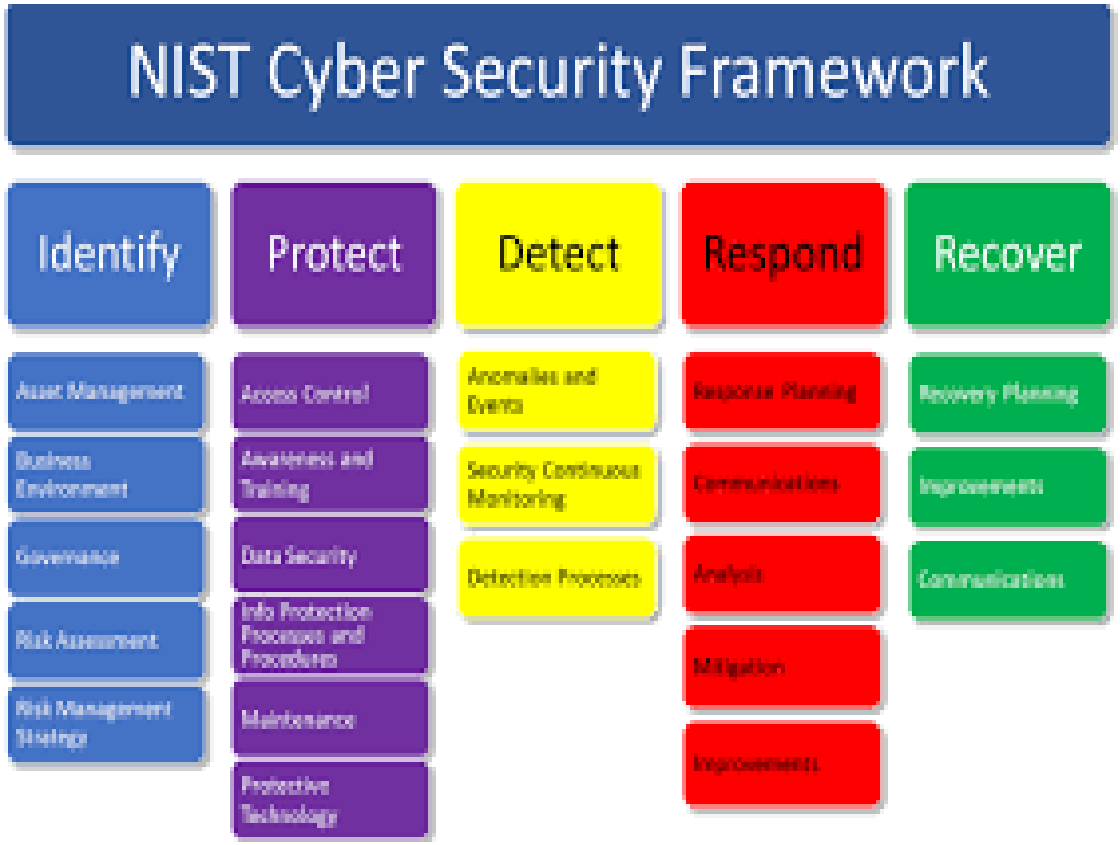
- **Lack of information results in uncertainty**
- **The amount of potential loss**

Mitigate Risk Exposure

Reduce unexpected business recovery expenses
Minimize technology losses and expenses
Minimize financial losses
Minimize intellectual property losses
Decrease liability costs due to products being cyber threat hosts
Avoid spending money on unusable/unneeded tools
Avoid failure to meet regulatory requirements or government compliance
Identify where security risks are possible/probable
Reduce negligence in protecting assets
Improve executive decision making
Increase knowledge of cyber law
Define public relations plan to prepare for an inevitable security breach
Cyber security needed down to the Internet of Things IoT level

Start With NIST Cyber Framework

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**



http://www.nist.gov/cyberframework/

NIST Cyber Framework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Stronger Cyber Security

1. **Prioritize and Scope**
2. **Orient**

   To related systems and assets, regulatory requirements, and overall risk approach. Then identify threats to, and vulnerabilities of, those systems and assets.
3. **Create a current profile**
4. **Conduct a risk assessment**
5. **Create a target Profile**
6. **Determine, analyze and prioritize the gaps**
7. **Implement action plan**

GENEDGE Risk Process

1. Establish the context
2. Conduct Risk Assessment
3. Implement Risk Treatment
4. Communicate and Consult
5. Monitor and review the risks and controls

Supply Chain Risks

External, End-to-End Risks

Supplier

Distribution

Internal Enterprise

Risk Mitigation

Cyber disaster planning and recovery – reduce the risk

Supply chain partners – transfer the risk

Security policies and training – avoid the risk

Cyber insurance

Cyber attorneys

Leading Virginia Cyber Companies

The Virginia-based firms listed on the Cybersecurity 500, Q2 2015 edition, in the order in which they appear are:

- 16. **Sera-Brynn**, cyber risk management, Suffolk, Va
- 64. **IKANOW**, threat analytics platform, Reston, Va
- 76. **Lookingglass**, cyber threat intelligence management, Arlington Va
- 81. **Leidos**, anti-terrorism and Homeland Security, Reston, Va
- 109. **Xceedium**, privileged identity management, Herndon, Va
- 127. **CYREN**, Web email and mobile security, McLean, Va
- 139. **CyFIR**, digital forensics and eDiscovery, Manassas, Va
- 146. **ePlus Security**, infosecurity products and services, Herndon, Va
- 151. **Haystax**, advanced threat analytics, McLean, Va
- 189. **Syntegrity Networks**, identity management and data security, Fairfax, Va
- 192. **ThreatSim**, proactive phishing defense, Herndon, Va
- 208. **Centripetal Networks**, cyber threat intelligence, Herndon, Va
- 215. **Cigital**, application security testing, Dulles, Va
- 220. **Ntrepid**, secure network and online computing, Herndon, Va
- 223. **Paraben**, digital forensics and data recovery, Ashburn, Va
- 224. **MindPoint Group**, IT security solutions, Springfield, Va
- 235. **Oberthur Technologies**, digital security for mobility, Chantilly, Va
- 238. **Northrop Grumman**, cyber and Homeland Security, McLean, Va
- 269. **CACI**, intelligence, defense and federal security, Ballston, Va
- 290. **MicroStrategy**, mobile identity platform, Tysons Corner, Va
- 312. **Daon**, identity assurance and biometrics, Fairfax, Va
- 331. **Vistronix**, cybersecurity for federal agencies, Reston, Va
- 345. **L-3**, national security solutions, Reston, Va
- 366. **Defense Point Security**, cybersecurity for federal agencies, Alexandria, Va
- 374. **CSC**, IT security services, Falls Church, Va
- 391. **SAIC**, cybersecurity professional services, McLean, Va
- 403. **Endgame**, security intelligence and Analytics, Arlington, Va
- 406. **Siemens Government Technologies**, cybersecurity for federal government, Arlington, Va
- 434. **Taia Global**, cybersecurity consulting services, McLean, Va
- 438. **AXON Ghost Sentinel**, Internet of Things security, Harrisonburg, Va
- 440. **Hyperion Gray**, open source Web security, Arlington, Va
- 446. **Veris Group**, cybersecurity professional services, Vienna, Va
- 451. **ThreatConnect**, cyber threat intelligence platform, Arlington, Va
- 461. **GuidePoint Security**, information security services, Reston, Va
- 465. **Risk Based Security**, cyber risk analytics, Richmond, Va
- 469. **SurfWatch Labs**, cyber risk intelligence analytics, Sterling, Va
- 478. **Paladion**, cybersecurity testing and monitoring, Herndon, Va
- 483. **Distil Networks**, malicious bot detection and prevention, Arlington,Va
- 495. **CloudHASH Security**, enterprise endpoint security, Fairfax, Va

Summary

- IoT is a HUGE and GROWING market
- If you are playing, you are a target
- Compliance and Regulatory issues uncertain and growing
- Ignore security at your peril
- There are ways to get help

Thank You For Your Interest

Roy Luebke

Email: rluebke@genedge.org

Cell: 276-732-8372