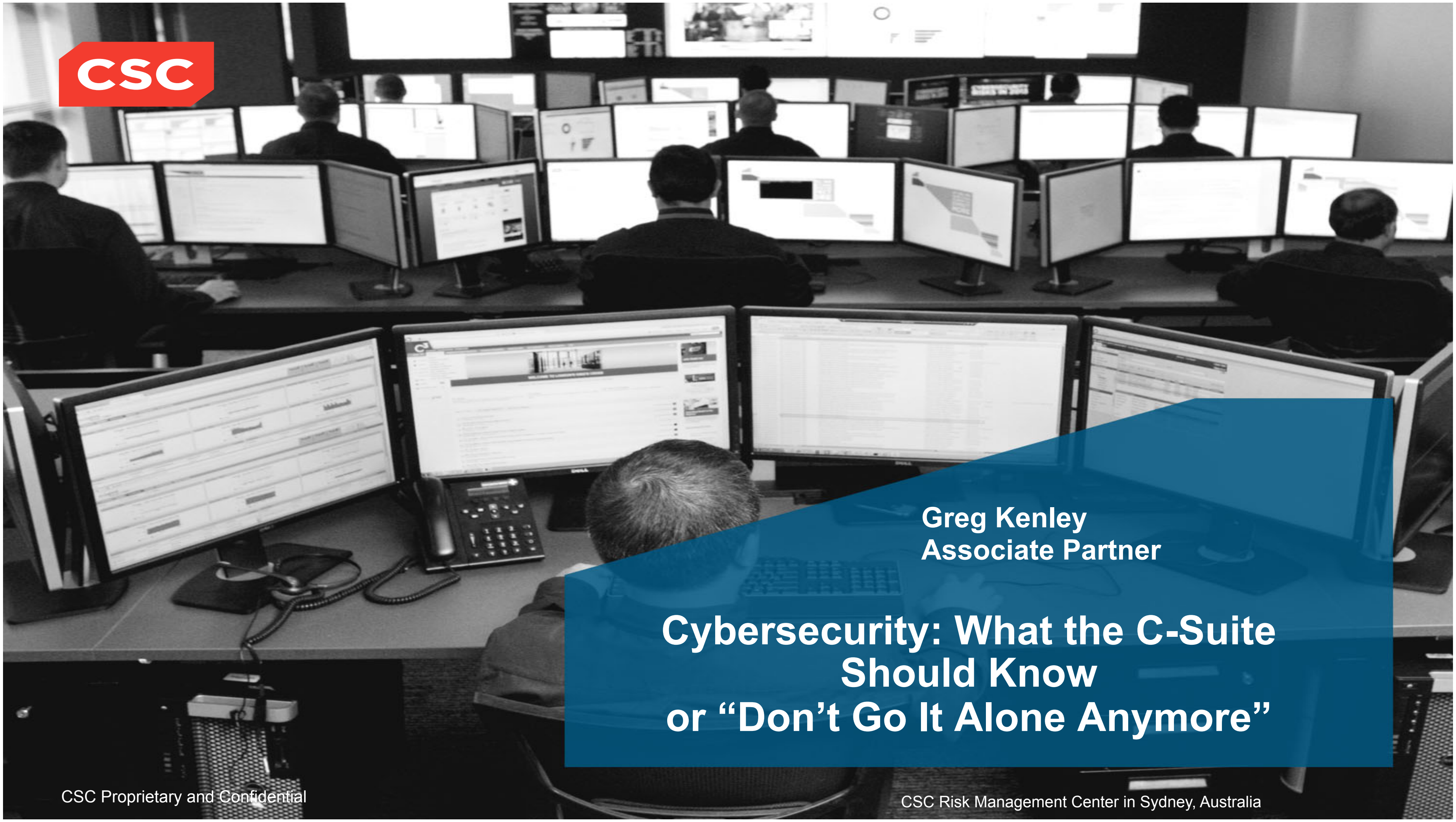


Greg Kenley
Associate Partner

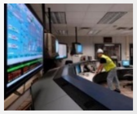
Cybersecurity: What the C-Suite Should Know or "Don't Go It Alone Anymore"

CSC Risk Management Center in Sydney, Australia

Agenda

What is Cyber

- Information Technology is the infrastructure that supports an organization’s computing environment
- Cyber is the larger environment, or ecosystem, of this IT environment as it connects to everything else and provides services
- Cyber includes:
  - Smartgrid Technology
  - Mobility
  - The Cloud
  - An organization’s computing environment as it connects to the world



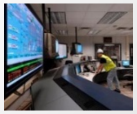
Current Landscape

2015

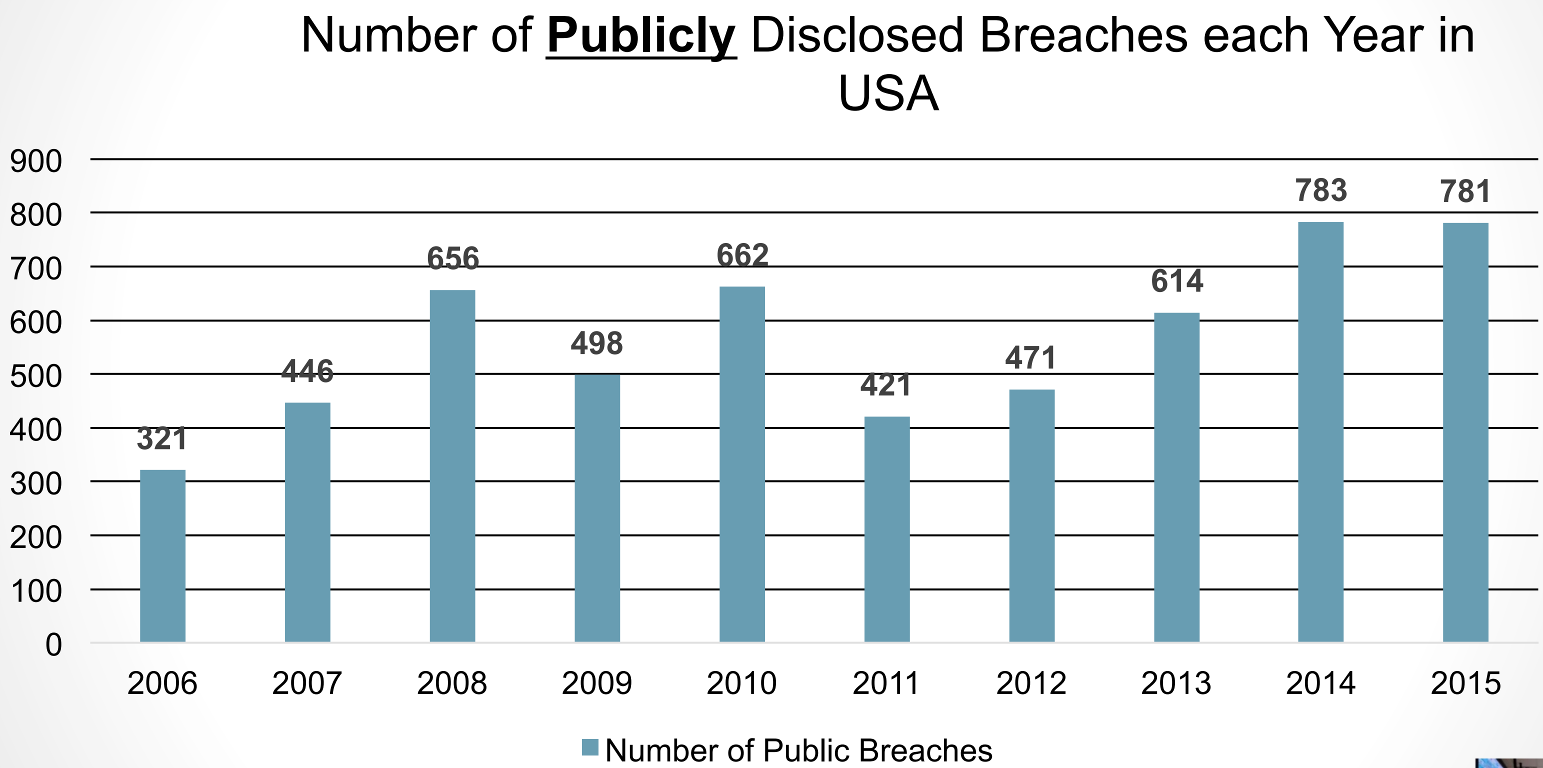
- Recorded 781 data breaches
- Exposed 169,068,506 records containing PII

2016 (so far)

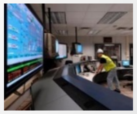
- Approximately **741** attacks recorded through August 31.
- Averaging 100 new breaches per month



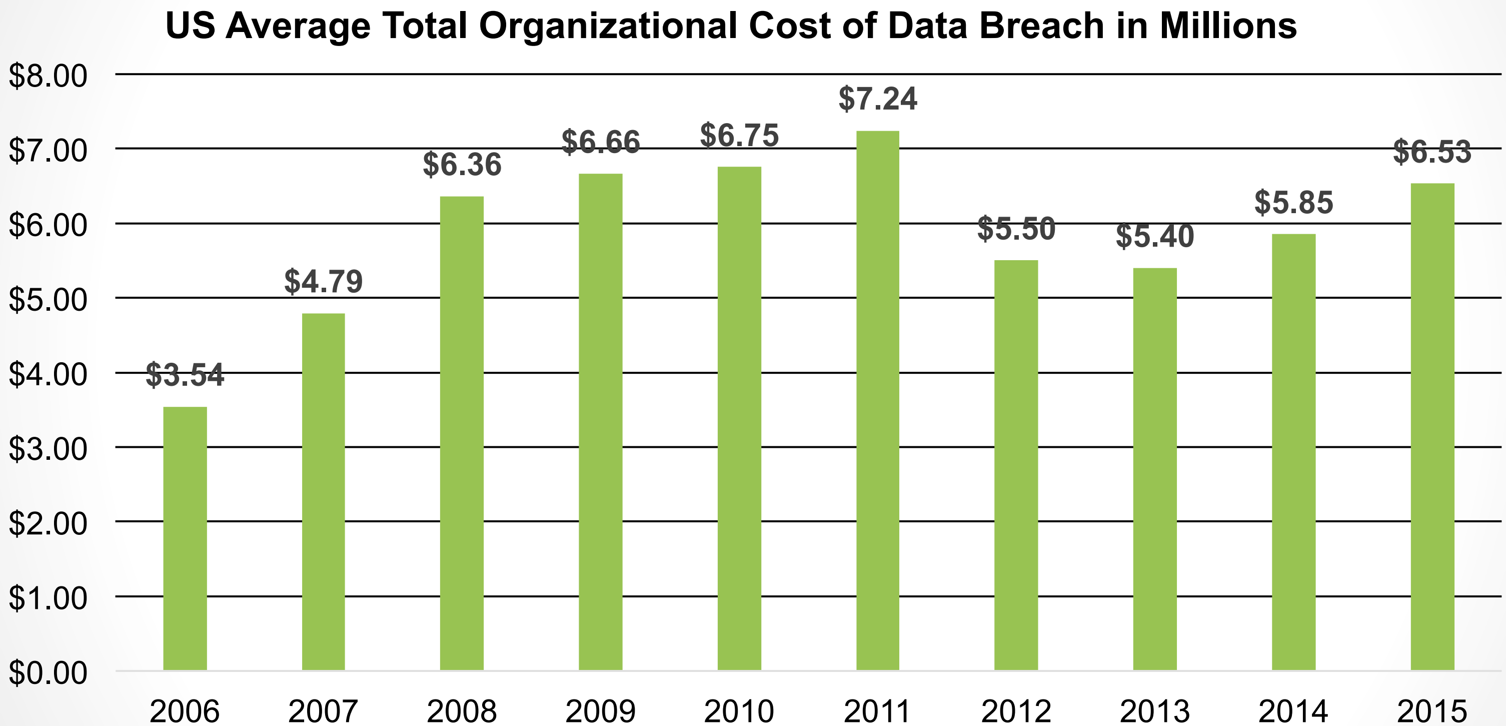
Last 10 Years



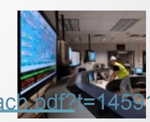
Source: Identity Theft Resource Center http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html



What Does That Mean in $?



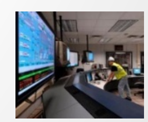
Projected global cost of cyber attacks for 2019 are $2.1 Trillion



* Ponemon 2015 Cost of Data Breach Study: United States. http://cdn2.hubspot.net/hubfs/360304/2015_Cost_Of_Data_Breach.pdf?t=1453177737613

Key Threats

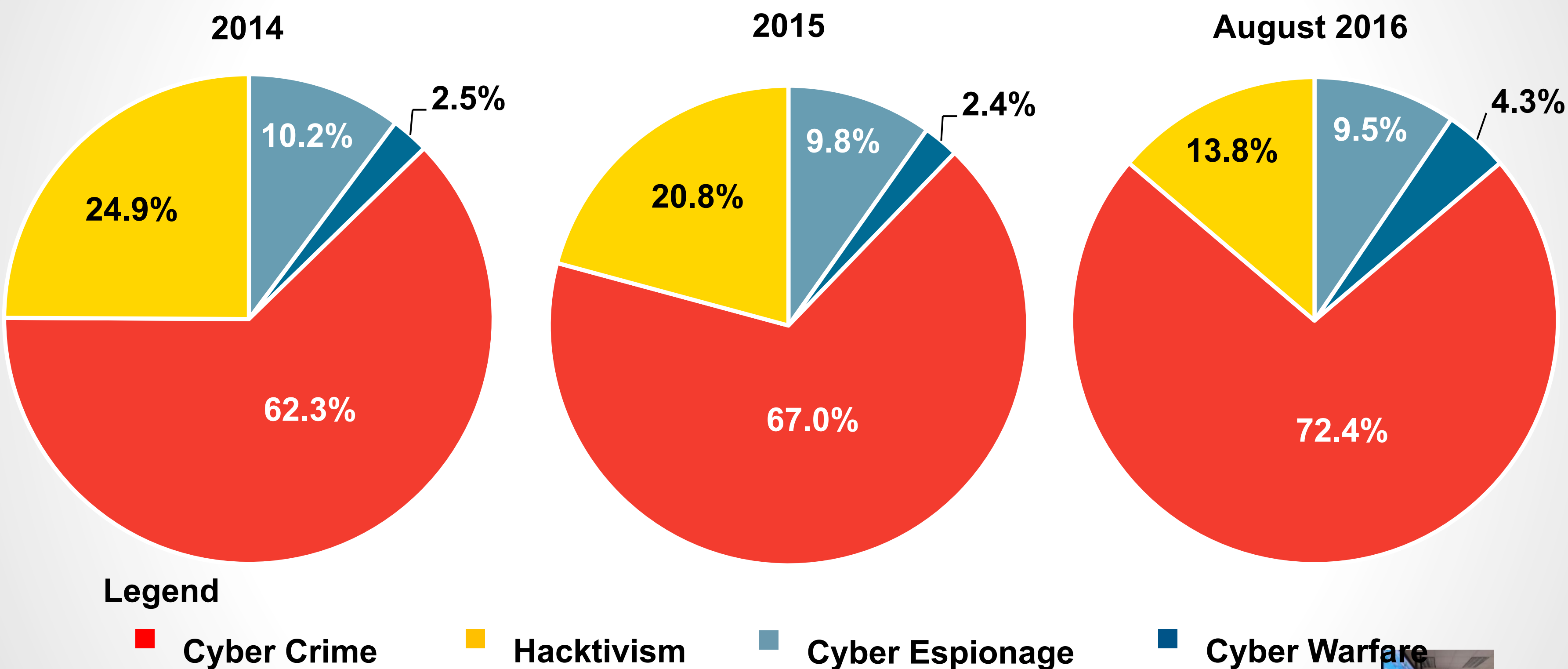
- Ransomware & (Medical Devices)
- Advanced Persistent Threats (APT)
- Zero Day Attacks
- **Phishing Attacks & Social Engineering**
- Attacks on Payment Systems
- Attacks on Cloud Systems
- Wearables and Consumer Goods (IoT)
- Mobile Security & Smartphone Vulnerability Threats

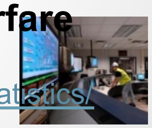


What’s the Difference?

- **Hacking** – Breaking through a vulnerability & moving laterally
- **APT** – “Uninvited Guest”
  - –Arrive into your network and stays there under the radar
  - –Harvesting information over time
  - –Typically not found with anti-virus software.
- **Malware** – Code that is designed to do bad things
  - –Execution of malicious code on an infrastructure
  - –Escalate unauthorized privileges
  - –Shut down your network (DDOS)
  - –Encrypt key data (Ransomware)

Motivations Behind Cyber Attacks
(all industries)



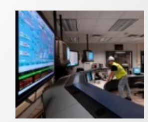


Source: Hackmageddon, http://www.hackmageddon.com/category/security/cyber-attack-statistics/

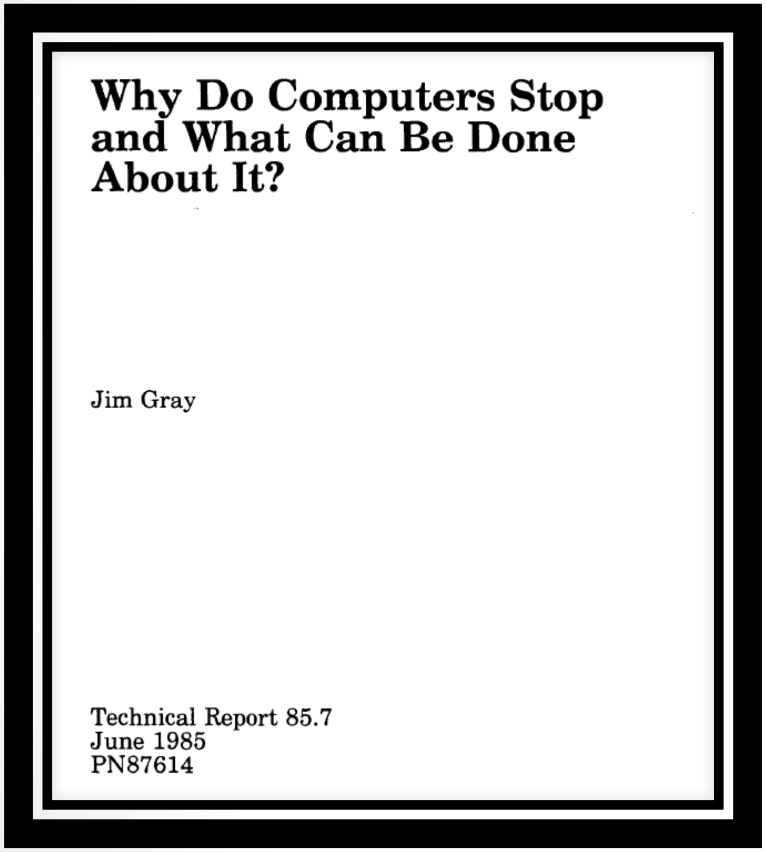
Cyber Defense
Primary Foundation

- Basic Tools
  - Firewalls
  - IPS/IDS
- Security Controls (ISO 27000, NIST 800-53, SANS)
- Policies, Standards & Procedures
- CMDB – SANs 1&2
- Monitoring
  - Logs/SIEM
  - Digital Asset Management
  - Social Media Management

This is good, but it only goes so far…



We Need a Game Change – A "New Order"



Why Do Computers Stop and What Can Be Done About It?

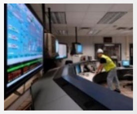
Jim Gray

Technical Report 85.7
June 1985
PN87614

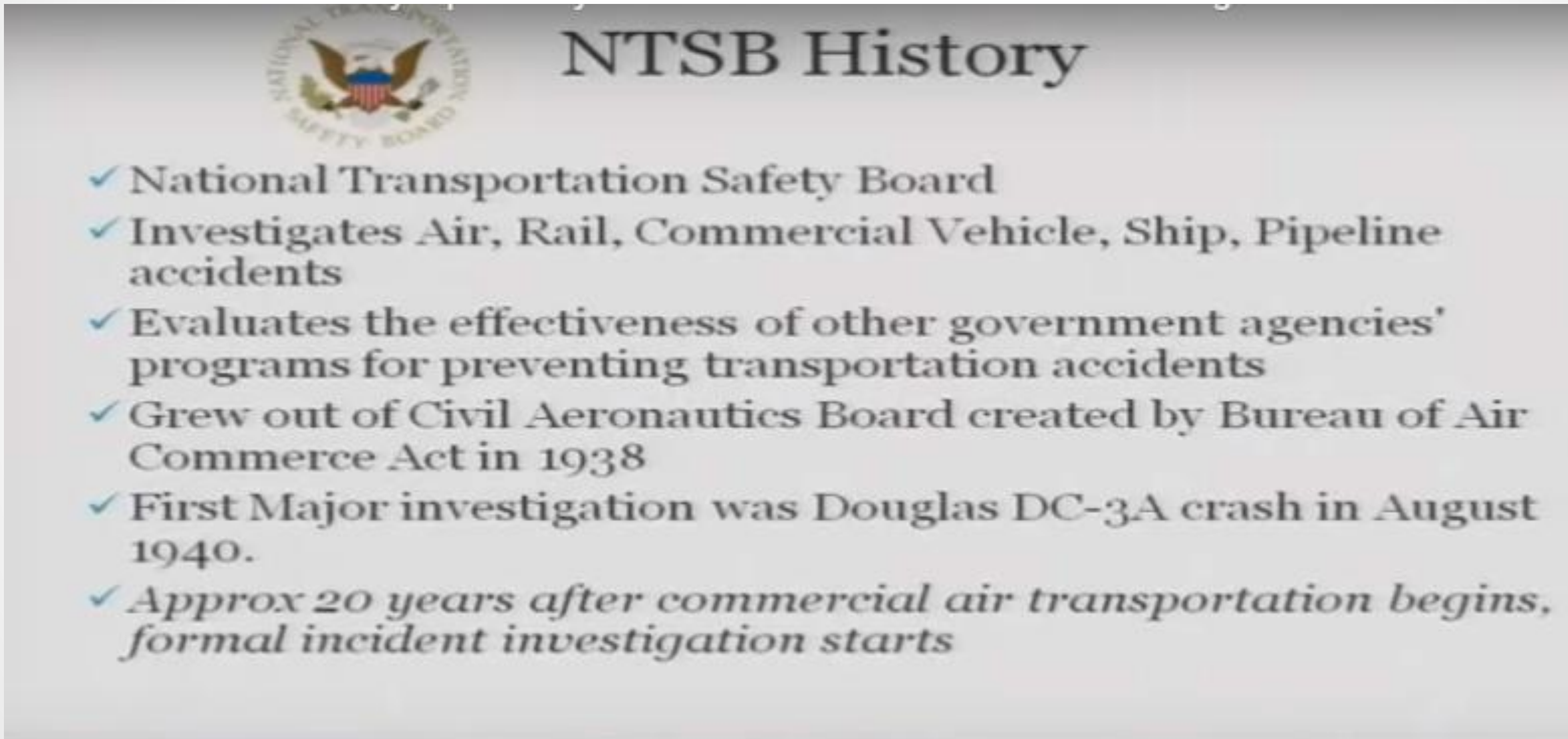
Source: Verizon DBIR

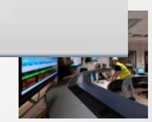
“Those Who Do Not Know History”… We’re Seen This Movie Before

RVAsec 2013: Chris Wysopal -- Keynote: Future of Government Info Sharing

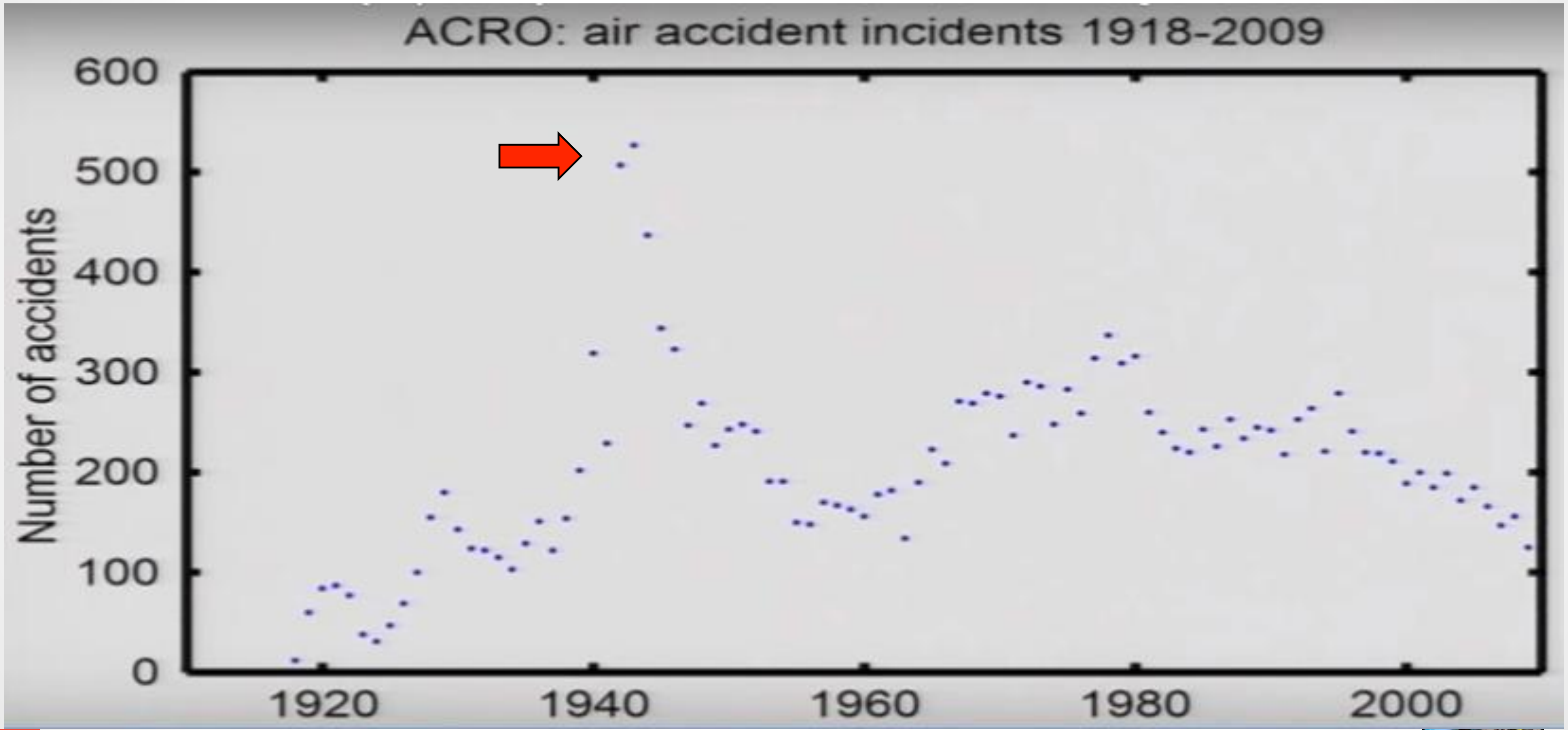


20 Years Later – 1940 - NTSB Formed





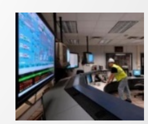
Accidents Dropped After Centralized NTSB Agency Created Everyone Report and Share Incident Data



NTSB Mandates The Submission Of Incident Reports
Central Repository of Shared Incident Information

NTSB Incident Reports

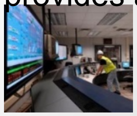
- ✓ Designed to learn from incidents and Improve
- ✓ Root cause analysis
- ✓ Recommendations
- ✓ Public Investigation for serious incidents
- ✓ Follows sound engineering principle of learning from failures.



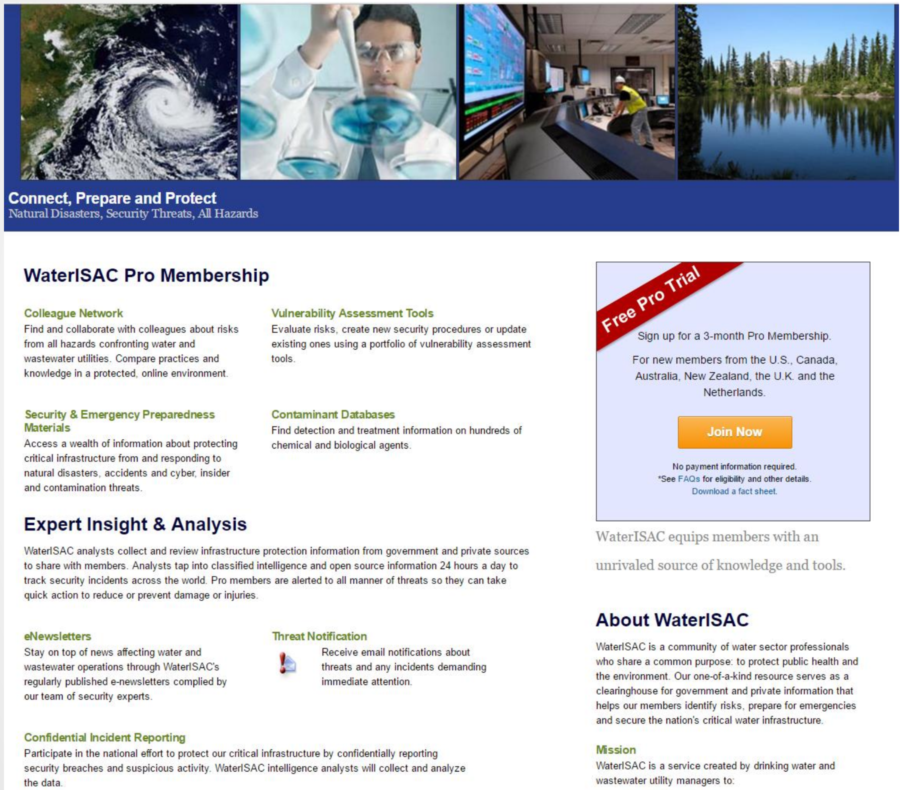
EO13636 - Executive Order issued Feb 12, 2013

"Improving Critical Infrastructure Cybersecurity"

- Risk Based Cybersecurity Framework – NIST CSF
  - Set of Industry Standards and Best Practices – Manage Cybersecurity Risks
  - Using **Business Drivers** to Guide Cybersecurity Activities
  - Critical Infrastructure was defined as Systems and Assets vital to USA:
    - Security
    - National Economic Security
    - National Public Health and Safety
  - Framework Core – five concurrent and continuous Functions
    - **Identify, Protect, Detect, Respond and Recover**
    - **Framework Profiles** – Current -> Target -> Future State
  - EO 13636 also recommend better use of Industry focused Cybersecurity **Information Sharing and Analysis Centers - ISACs**
    - for each of the nation's critical infrastructures, there is an Information Sharing & Analysis Center (ISAC) – Financial Services, IT, **WaterISAC**(2002), Communications, Supply Chain, Transportation, Real Estate, Nuclear, Electric, Healthcare
    - What is an "ISAC"? An Information Sharing and Analysis Center is a nonprofit organization that provides a **central resource for gathering information** on cyber threats to critical infrastructure.



WaterISAC – Established in 2002 – Centralized Information Sharing Specific to Industry



Connect, Prepare and Protect
Natural Disasters, Security Threats, All Hazards

WaterISAC Pro Membership

Colleague Network
Find and collaborate with colleagues about risks from all hazards confronting water and wastewater utilities. Compare practices and knowledge in a protected, online environment.

Vulnerability Assessment Tools
Evaluate risks, create new security procedures or update existing ones using a portfolio of vulnerability assessment tools.

Security & Emergency Preparedness Materials
Access a wealth of information about protecting critical infrastructure from and responding to natural disasters, accidents and cyber, insider and contamination threats.

Contaminant Databases
Find detection and treatment information on hundreds of chemical and biological agents.

Expert Insight & Analysis

WaterISAC analysts collect and review infrastructure protection information from government and private sources to share with members. Analysts tap into classified intelligence and open source information 24 hours a day to track security incidents across the world. Pro members are alerted to all manner of threats so they can take quick action to reduce or prevent damage or injuries.

eNewsletters
Stay on top of news affecting water and wastewater operations through WaterISAC's regularly published e-newsletters complied by our team of security experts.

Threat Notification
Receive email notifications about threats and any incidents demanding immediate attention.

Confidential Incident Reporting
Participate in the national effort to protect our critical infrastructure by confidentially reporting security breaches and suspicious activity. WaterISAC intelligence analysts will collect and analyze the data.

Free Pro Trial

Sign up for a 3-month Pro Membership.

For new members from the U.S., Canada, Australia, New Zealand, the U.K. and the Netherlands.

Join Now

No payment information required.
*See FAQs for eligibility and other details.
Download a fact sheet.

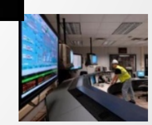
WaterISAC equips members with an unrivaled source of knowledge and tools.

About WaterISAC

WaterISAC is a community of water sector professionals who share a common purpose: to protect public health and the environment. Our one-of-a-kind resource serves as a clearinghouse for government and private information that helps our members identify risks, prepare for emergencies and secure the nation's critical water infrastructure.

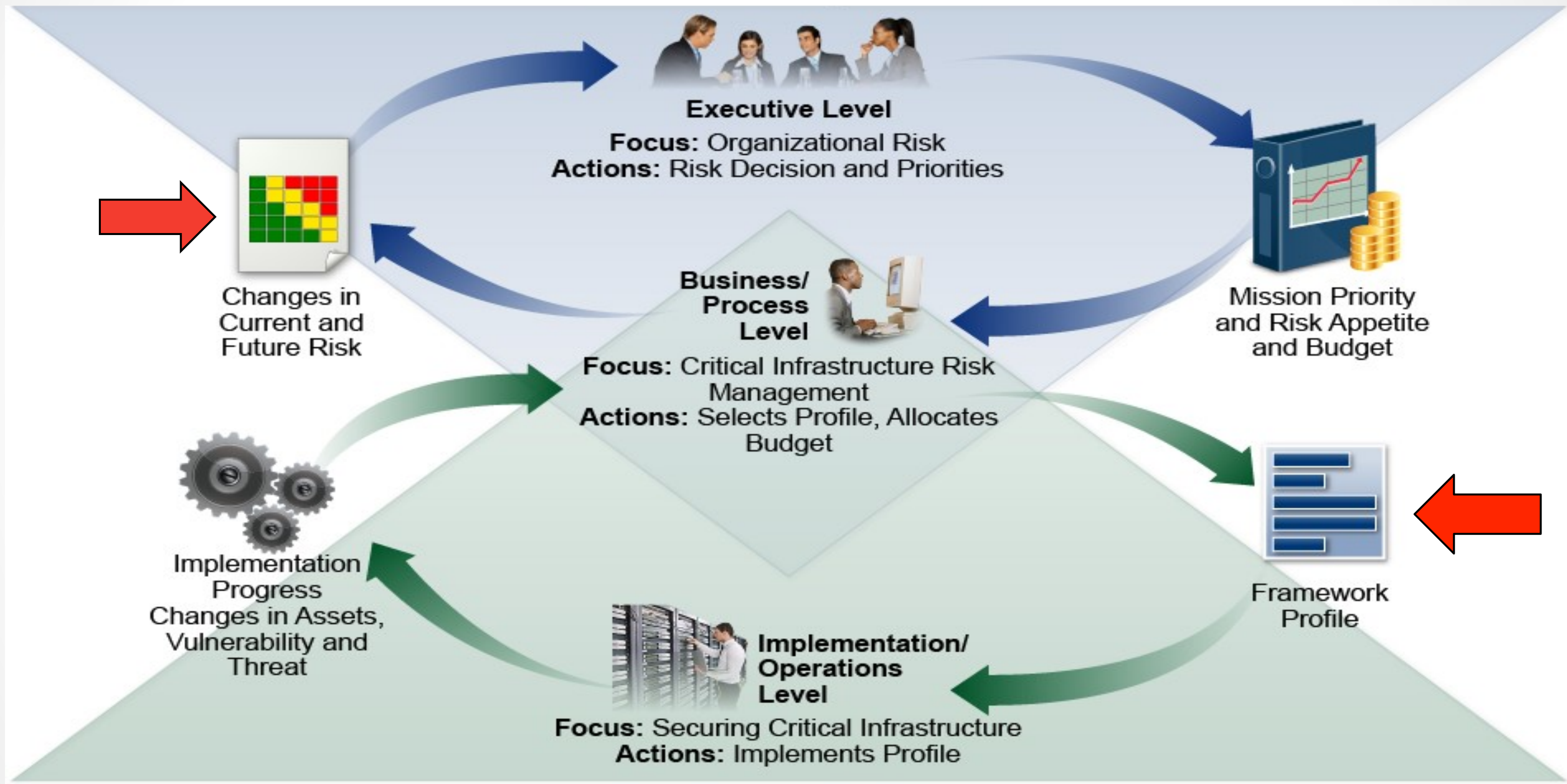
Mission
WaterISAC is a service created by drinking water and wastewater utility managers to:

Some ISACs are now **<u>sharing</u>** key SIEM Indicators to Members

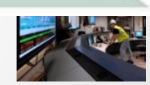


Cybersecurity Must Be Actioned at All Levels

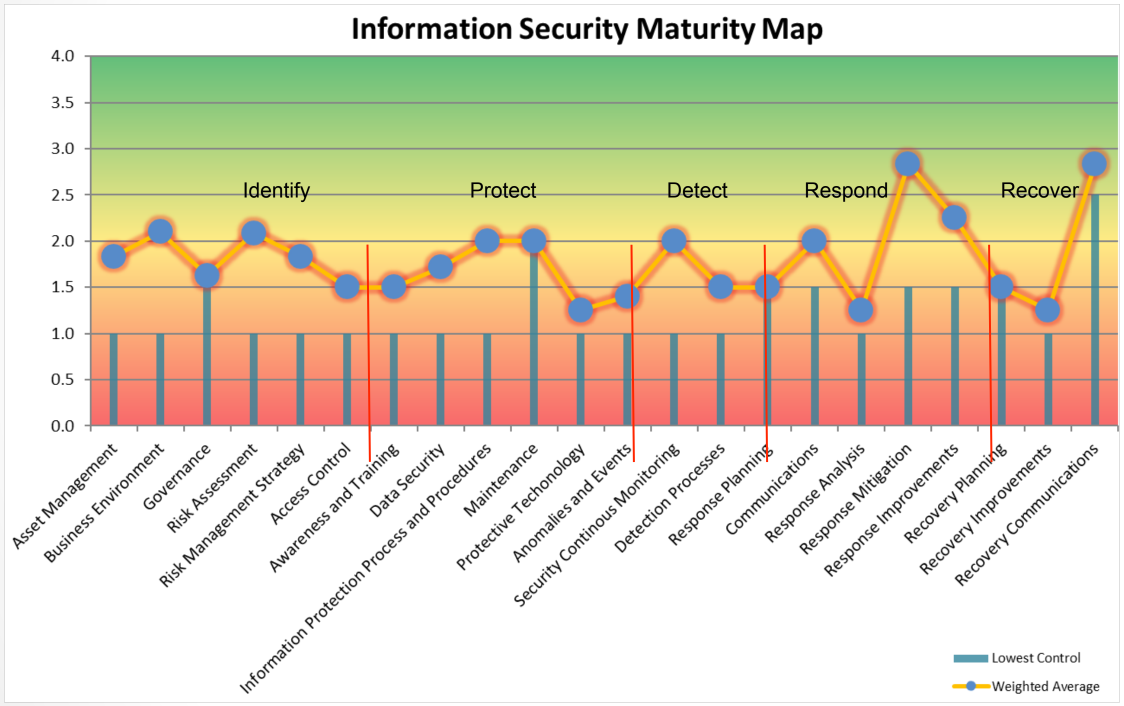
Defined, Repeatable Process – How to <u>Communicate</u> across 3 Levels?

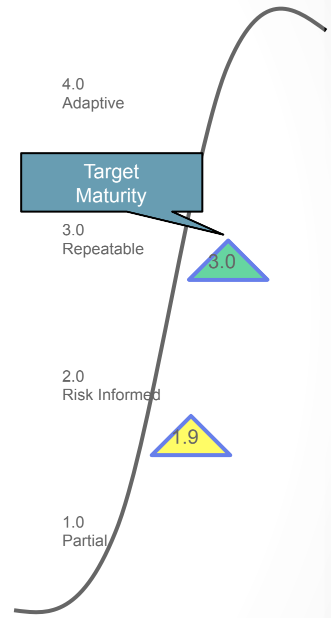


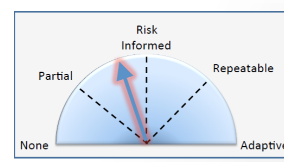
NIST Cyber Security Framework (CSF)

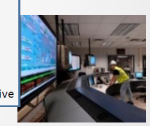


Security Framework Maturity
The Framework Profile









Fundamentals Are Essential BUT Require a Risk Based Approach
"Patch Tuesday = Patch Tsunami"

Effective patching can stop them

The top 10 vulnerabilities [Common Vulnerabilities and Exposures, or CVEs] accounted for 85% of successful exploit traffic. The other 15% comprises over 900 CVEs.

Patching promptly is important, but with so many new vulnerabilities being discovered, it's hard to know where to start. This year's DBIR provides valuable information to help you solve that problem.

Data provided by Kenna Security suggests that vulnerabilities in Adobe products were exploited quickest; ones in Mozilla products the slowest – see Figure 5. Studying this information will help you move away from conducting "fire drills" and focus your patching efforts.

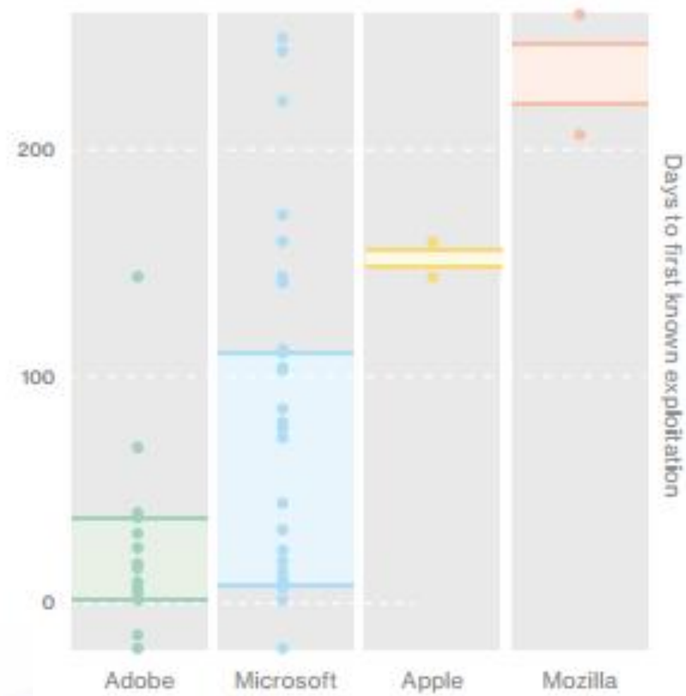
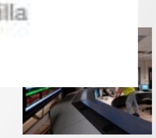


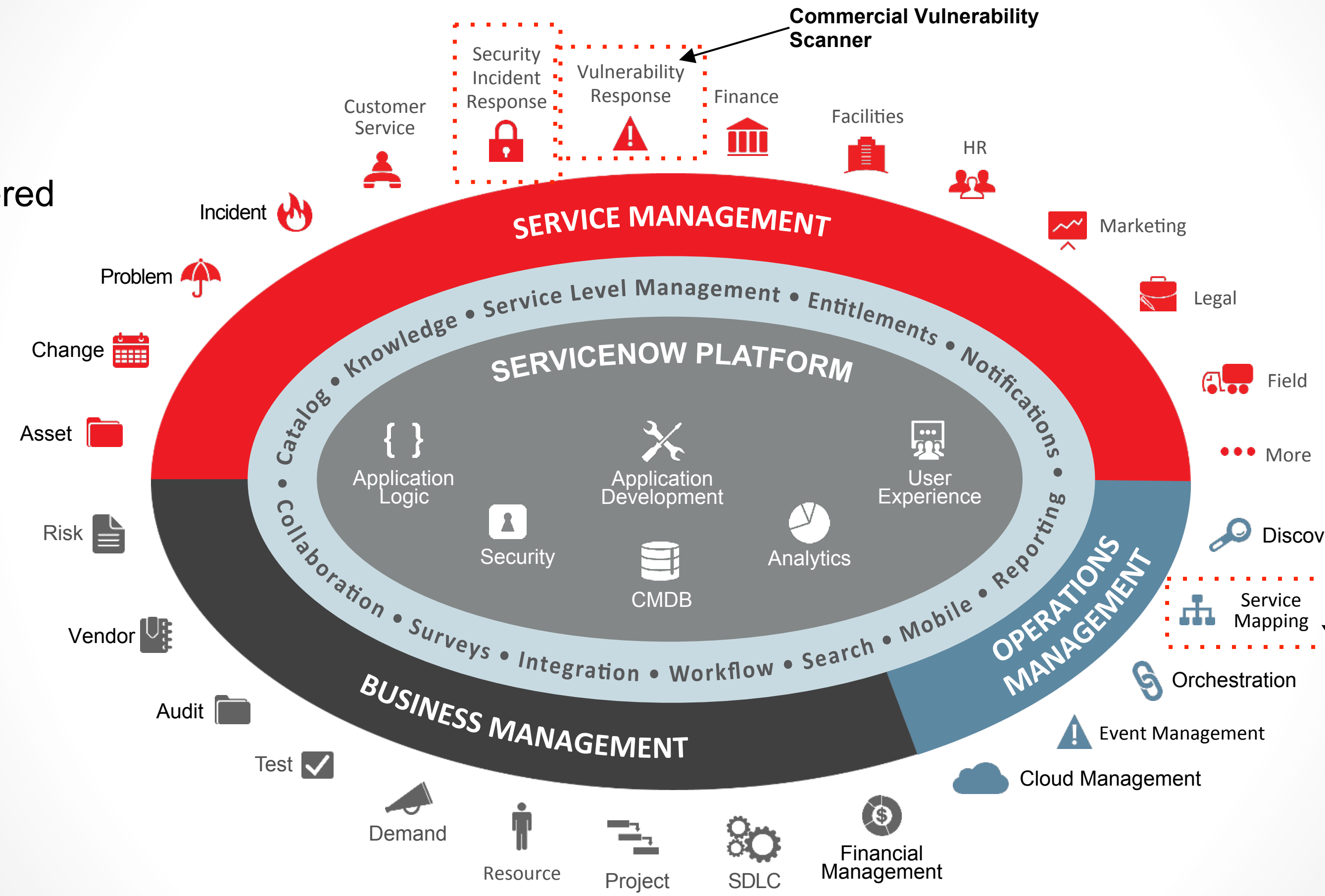
Figure 5: Days to first known exploitation

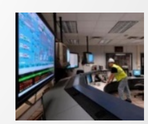


Source: Verizon DBIR

IT Service Management – Workflows – Delivered as a Cloud Service

Risk Based Vulnerability Process delivered as a Workflow





Game Change Requirement – Proactive vs Reactive

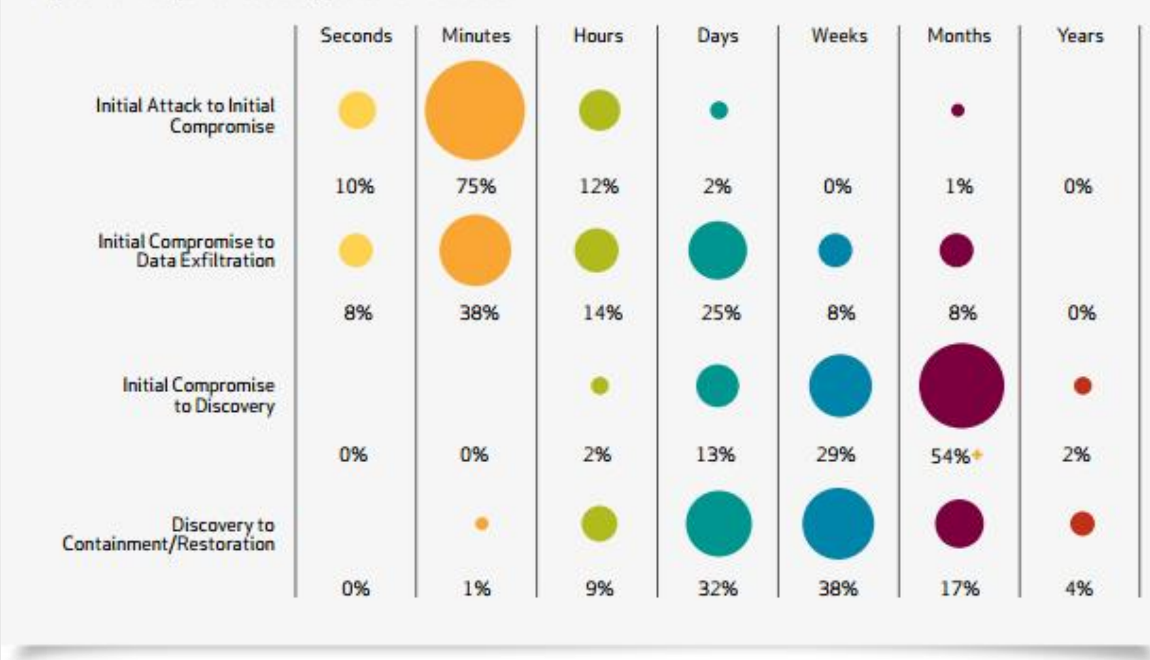
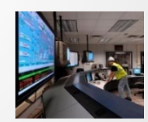


Figure 40. Timespan of events by percent of breaches

Breach Assessments:

"They're not just for known breaches anymore."

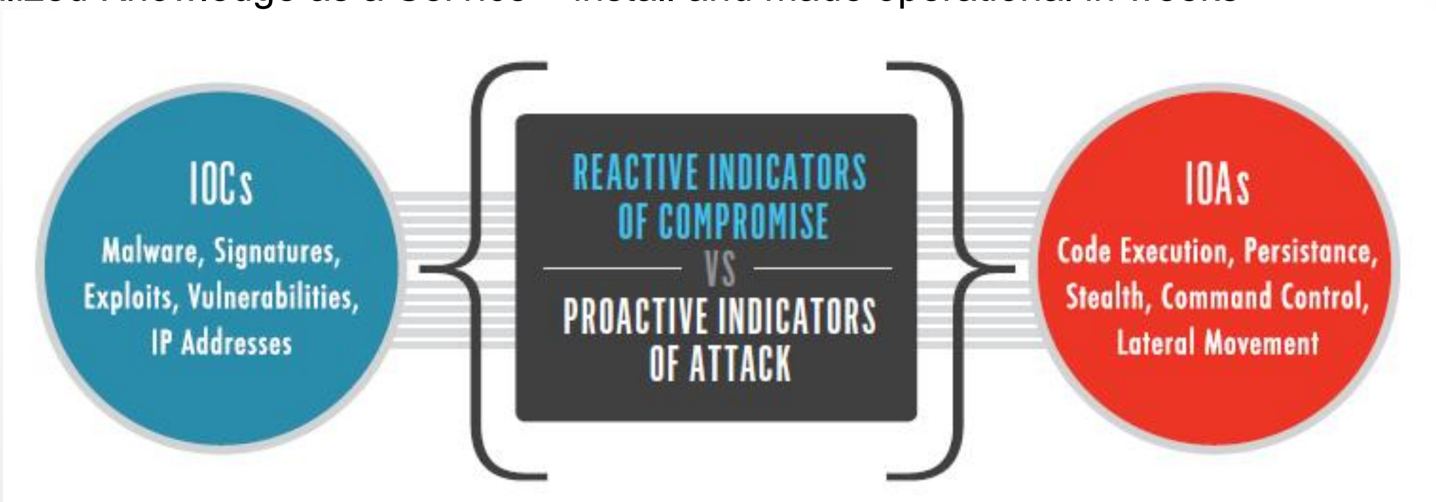
Post Ransomware – discovering that there were actually multiple actors that had taken residency.

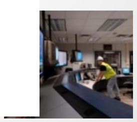


Source: Verizon DBIR

Endpoint Protection vs Enterprise Detection & Response (EDR) via a Cloud Service

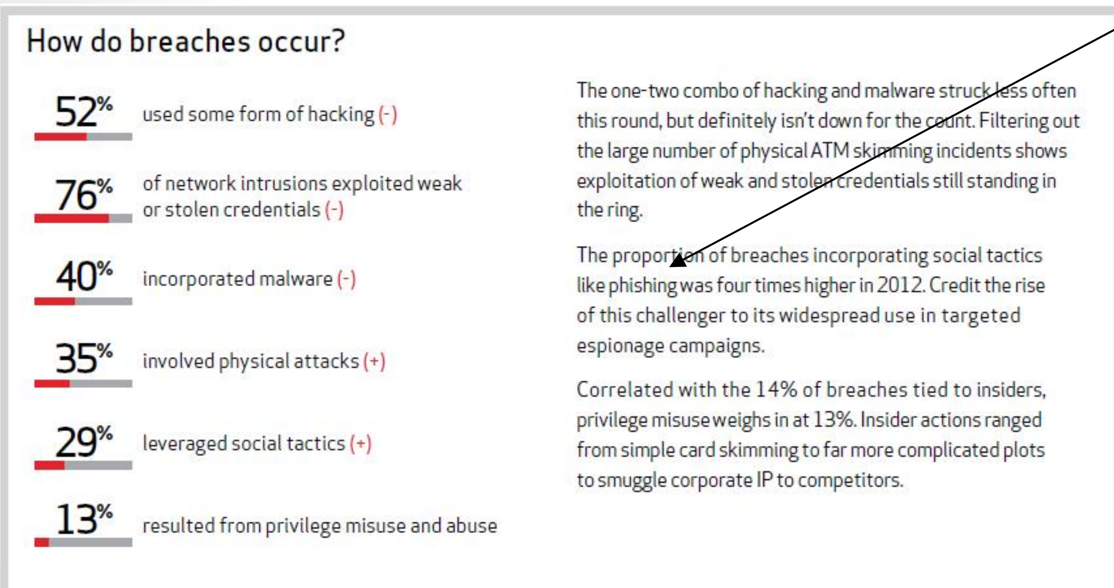
- Indicators of Compromise (IOC) constitute a **Reactive** posture
- Indicators of Attack (IOA) represent a **Proactive** stance – early warning signs of attack underway
- 60% of attacks no longer utilize Malware – must use behavior analysis and **Experience**
- Catalog of know Actors and their “trade craft” – team reverse engineering artifacts
- Tracking thousands of threat campaigns and logging their sequences and methodologies
- Provided as <u>shared knowledge as a Service </u>VS 1) Hire & Retain 2) Train for 1000s of campaigns
- Centralized Knowledge as a Service – install and made operational in weeks





Source: Verizon DBIR

The Rise of Social Engineering – Phishing gets more (too) effective
(Your) People are your new Perimeter


How do breaches occur?

52% used some form of hacking (-)

76% of network intrusions exploited weak or stolen credentials (-)

40% incorporated malware (-)

35% involved physical attacks (+)

29% leveraged social tactics (+)

13% resulted from privilege misuse and abuse

The one-two combo of hacking and malware struck less often this round, but definitely isn't down for the count. Filtering out the large number of physical ATM skimming incidents shows exploitation of weak and stolen credentials still standing in the ring.

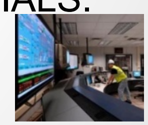
The proportion of breaches incorporating social tactics like phishing was four times higher in 2012. Credit the rise of this challenger to its widespread use in targeted espionage campaigns.

Correlated with the 14% of breaches tied to insiders, privilege misuse weighs in at 13%. Insider actions ranged from simple card skimming to far more complicated plots to smuggle corporate IP to competitors.

"Social tactics like phishing was four times higher in 2012"

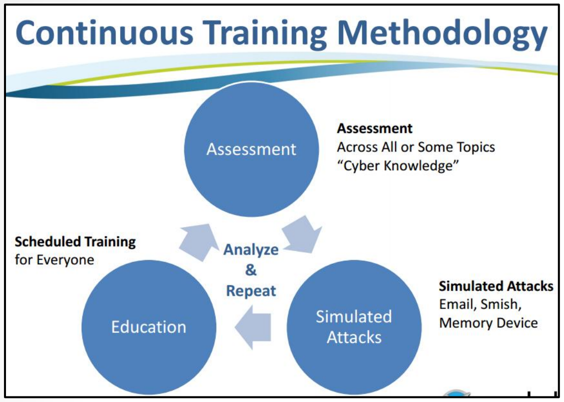
"Often the reason why criminals were so quick at breaking in was that they already had the key. Social engineering remains worryingly effective – "click here to reset your password". Almost a **third (30%)** of phishing messages were opened – up from 23% in 2014."

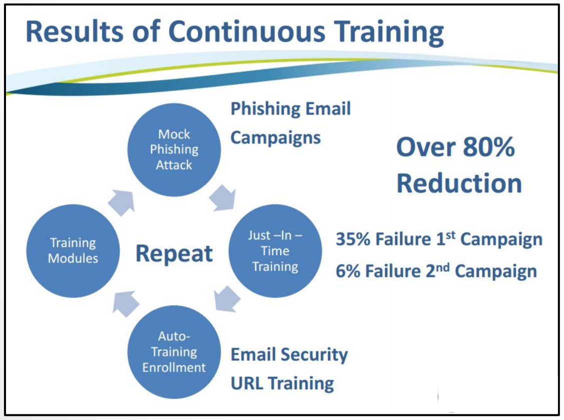
CSC Cybersecurity teams are now seeing typical cases where 30% GAIN FULL CREDENTIALS.

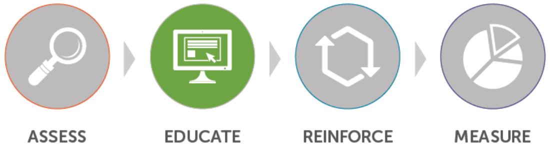


Source: Verizon DBIR

Continuous Training Methodology – Auto Scheduled "Teachable Moment" – Available as a Cloud Delivered Service

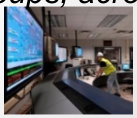






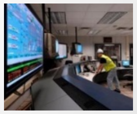
- *Interactive Scenario based training – engages users, educates employees to make the right decisions when faced with security threats. Facilities retention and behavior change*
- *Provide Targeted Training – by department, based on history*
- *Time efficient – each module is approximately 10-15 mins*
- *Consistent Global Training – 20 languages available*
- *Streamline Program Management – schedule assignments, track completion rates, set reminders and measure results all from a single interface*
- *Auto-Training enrollment – The "Teachable Moment"*

- ***The "yearly security training requirement" is not effective***. *Training needs to be applied based on actual results. How to track and auto report on effectiveness – across groups, across regions, across countries.*



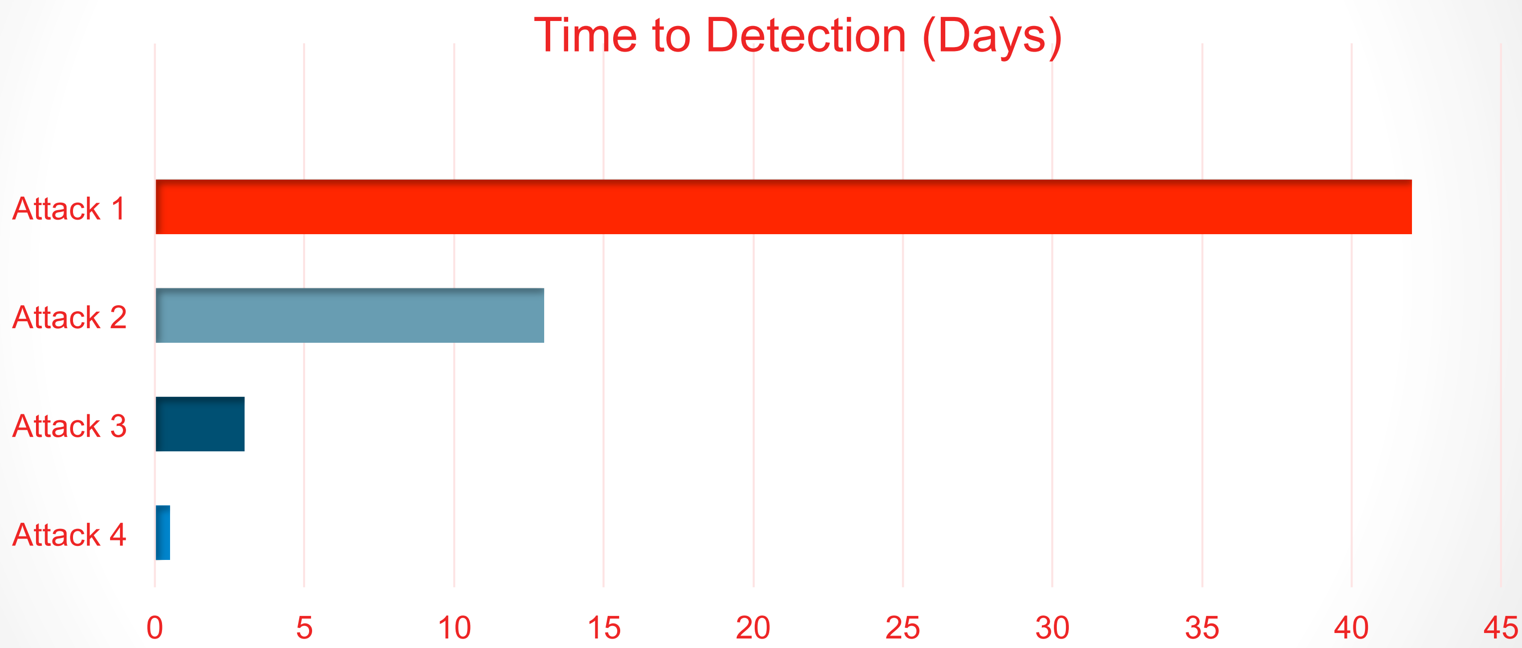
Cyber Defense
Next Level

- Defense Planning and Intelligence Gathering
  - Cyber Threat Intelligence (CINTEL) Subscription Services
  - Periodic Assessments
    - Social Engineering Assessments
    - Penetration Testing
    - Physical Security
    - Breach Assessments
    - Digital Attack Simulations (DAS) - new

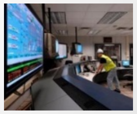


Example Proactive Project – Digital Attack Simulation (DAS)

Case Study: Fortune 300 Company Blue Team Improvements (12 Months)

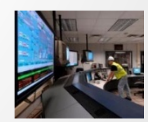


CURRENT GLOBAL AVERAGE "TIME TO DETECTION" IS APPROXIMATELY 200 DAYS.



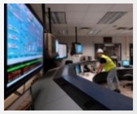
Benefits of the Simulation – Preparation vs Reaction

- Discovery of real world weaknesses in current security posture
- Identify unknown assets which pose a risk to the business
- Reduce the ‘time to detection’ of modern security threats



Importance of Defense Planning

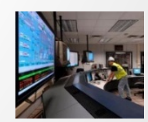
- Realistic assessments from credible third parties
- CINTEL - **Combined knowledge is greater than individual knowledge**
  - Relevant
  - Timely
  - Accurate
  - Actionable
- Preparation to allow mitigation



Cyber Defense
Next Level

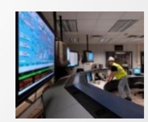
- Documented Response Plan
  - Incident Response Plan and Maintenance
  - Root Cause Analysis
  - Key Performance Indicators

  - Document the “Information Security Management System” (ISO 27000 ISMS) – it’s the “Root Security Document”



Takeaways and Considerations

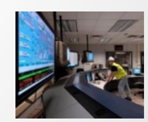
- Cyber breaches and incidents are occurring daily
- Plan for the breach, and set up a cyber defense
- Consider the **new leverage of Shared Knowledge** to defend your environment - **Proactively**
- Continually train your new perimeter – People not Firewalls
- Ensure your data is encrypted – DBMS
- Preparation (Incident Response Plan) will mitigate the impact



CSC

Questions?

?



Sources

McAfee Labs 2016 Threats Prediction Report

NY State Dept. of Financial Services: Report on Cyber Security in the Insurance Sector, Feb. 2015

SANS Institute: Who’s Using Cyberthreat Intelligence and How? Feb. 2015

Hackmageddon Information Security Timelines and Statistics http://www.hackmageddon.com/category/security/cyber-attacks-timeline/

National Association of Insurance Commissioners, Cybersecurity updated July 20, 2016 http://www.naic.org/cipr_topics/topic_cyber_risk.htm

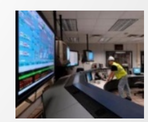
Computer Weekly, http://www.computerweekly.com/opinion/How-to-source-cyber-threat-intelligence

Verizon, 2012 - 2016 Data Breach Investigations Reports

NBC News, Feb. 13, 2016

Business Insurance, Jun. 5, 2015

Infoworld, Sep. 14, 2015



Thank You

Greg Kenley

Associate Partner

Cybersecurity Business Consulting

CSC

gkenley@csc.com