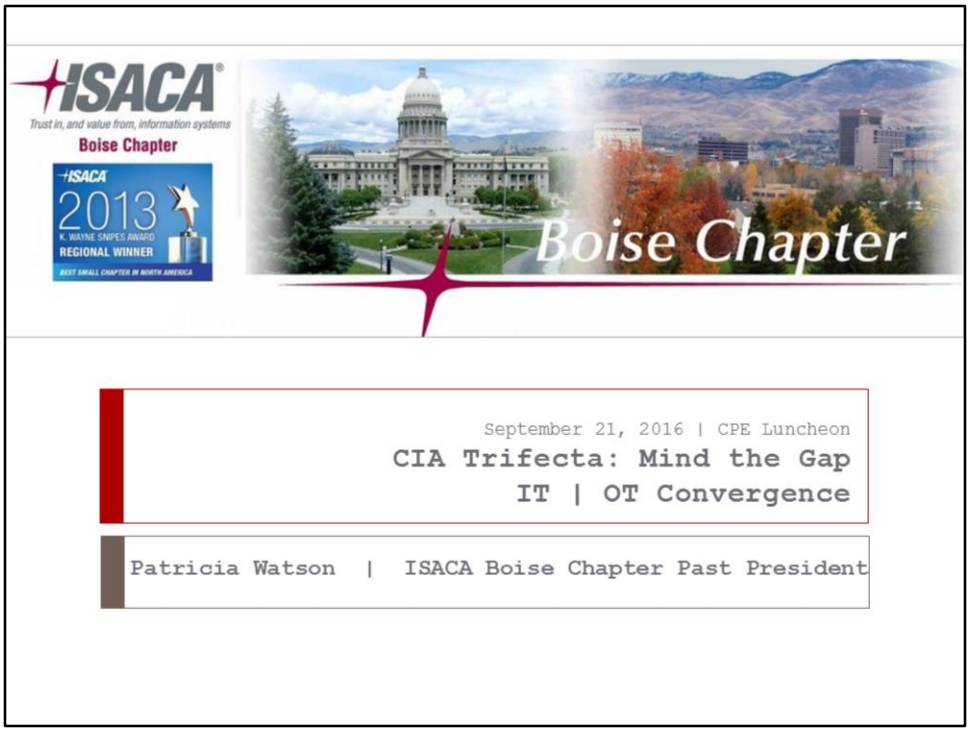


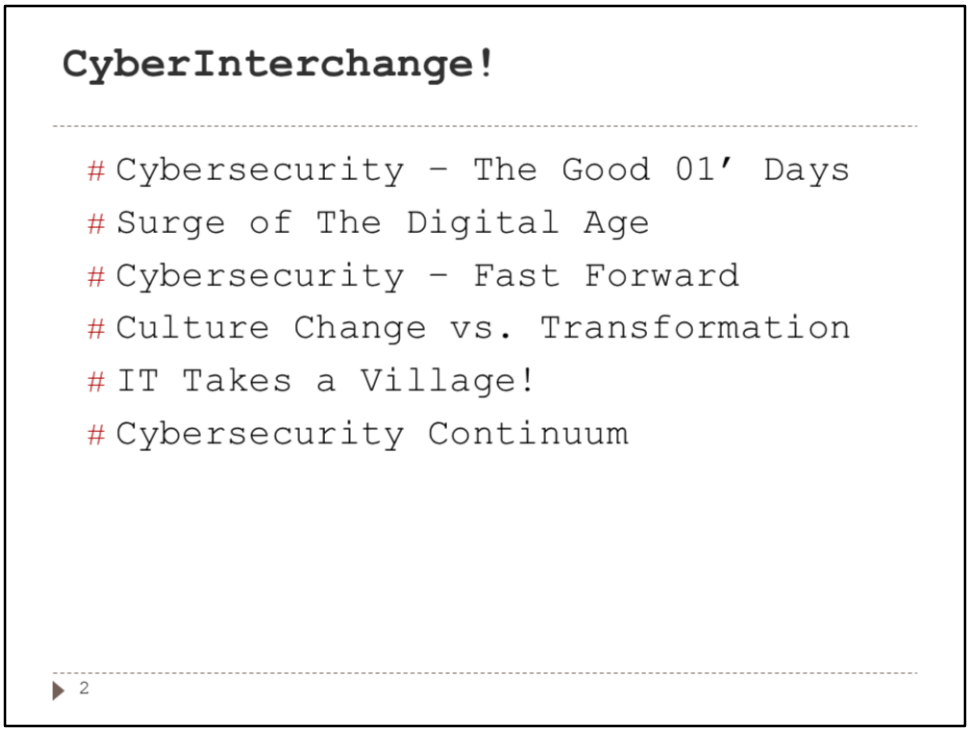
ISACA Boise Chapter CPE Luncheon

CIA Trifecta: Mind the Gap – IT | *OT Convergence

Presentation Synopsis:

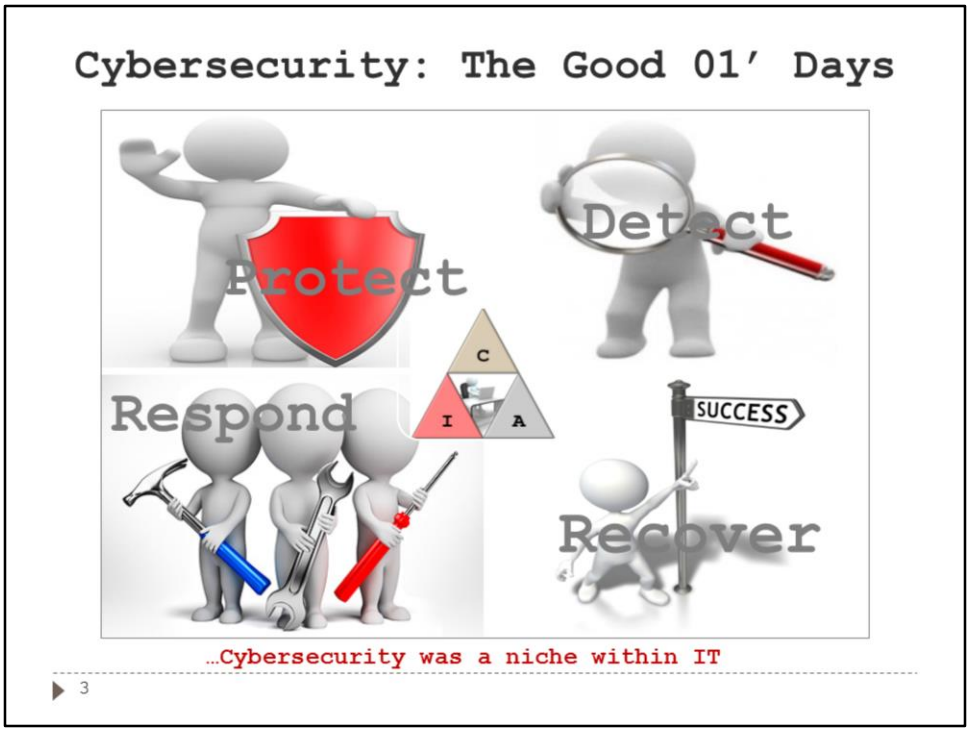
As eloquently stated by Peter Drucker…Culture eats strategy for breakfast! In this ever interconnected world, Cybersecurity has become an integral function for just about every business activity. While the CIA triad serves as a model that is diligently applied in the Cybersecurity landscape, operational functions mandate real-time expediency. Cross-functional collaboration and adaptation of the proverbial interconnected reality warrants a shift in the way we approach Cybersecurity solutions.

*In the context of this presentation, OT encompasses the business and/or administrative side of the house (all departments outside of IT/Cybersecurity)



As per the usual…Disclaimer

- Material discussed in this presentation are the views of the author
- This presentation is intended for discussion purposes, not to be relied upon as advice



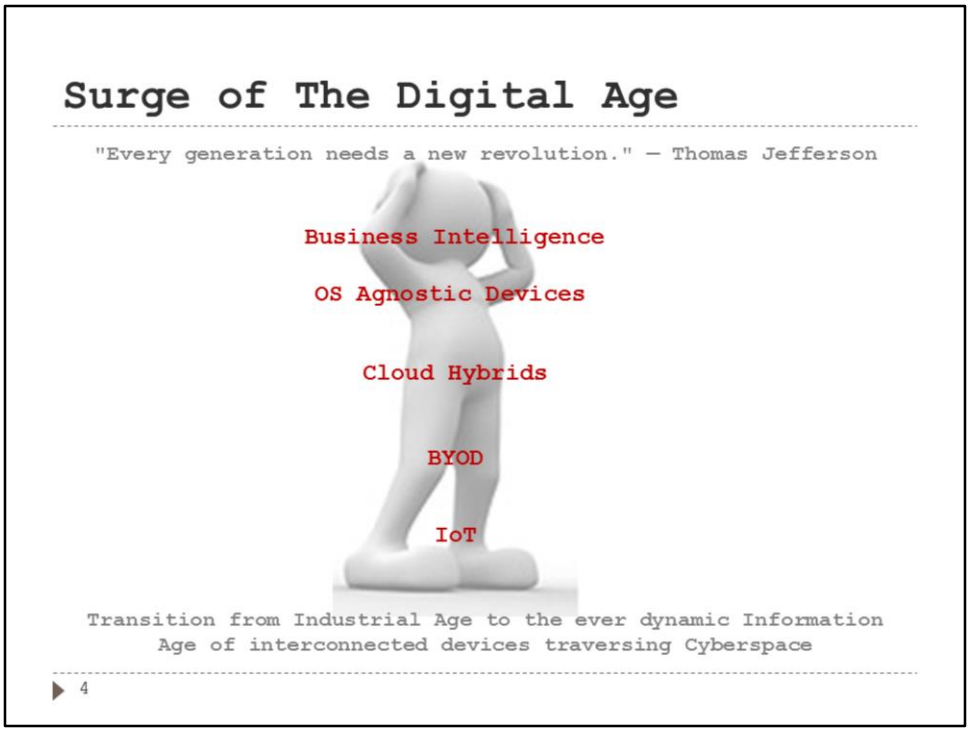
Discussion Summary – Cybersecurity: The Good Old Days

Back in the good old days…Cybersecurity was a niche within the IT field with the main objective to ensure Confidentiality, Integrity and Availability of data & systems

Static, proactive, preventive solutions that were housed in the company's data center (physical appliances)

A Few Examples Discussed:

SOC – Blue Team, Red Team
Network segmentation
DMZs
MS Active Directory Group Policy
Perimeter (network controls: IPS/IDS, firewalls, NAC, Web traffic, SIEM), Endpoint (AV, USB mgt, Data Loss Prevention (DLP))
Two factor authentication
Application and perimeter firewalls
To encrypt or not to encrypt
Cybersecurity Framework Function Areas



Discussion Summary – Surge of The Digital Age

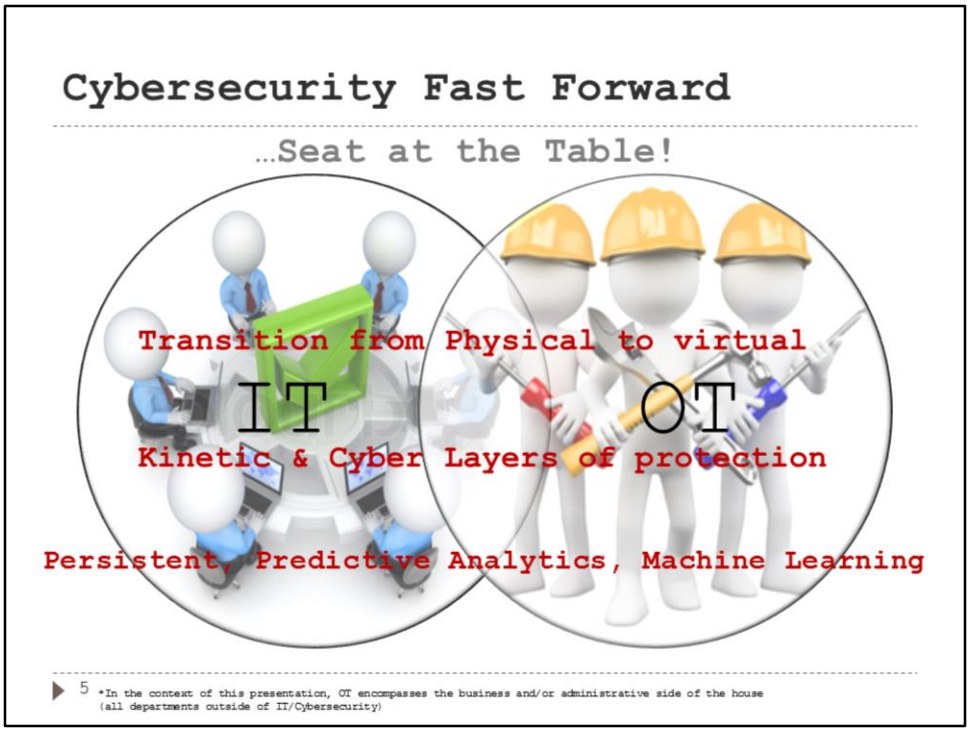
We've made the transition from the Industrial age to the ever dynamic information age of interconnected devices traversing cyberspace

Even if your company/firm is not directly engaging/leveraging the latest and greatest technology solutions, your customers, suppliers, vendors and competitor are…be ware!

A Few Examples Discussed:

Business Intelligence
OS Agnostic Devices
BYOD
IoT

Quote: Every generation needs a new revolution – Thomas Jefferson



Discussion Summary – Cybersecurity Fast Forward

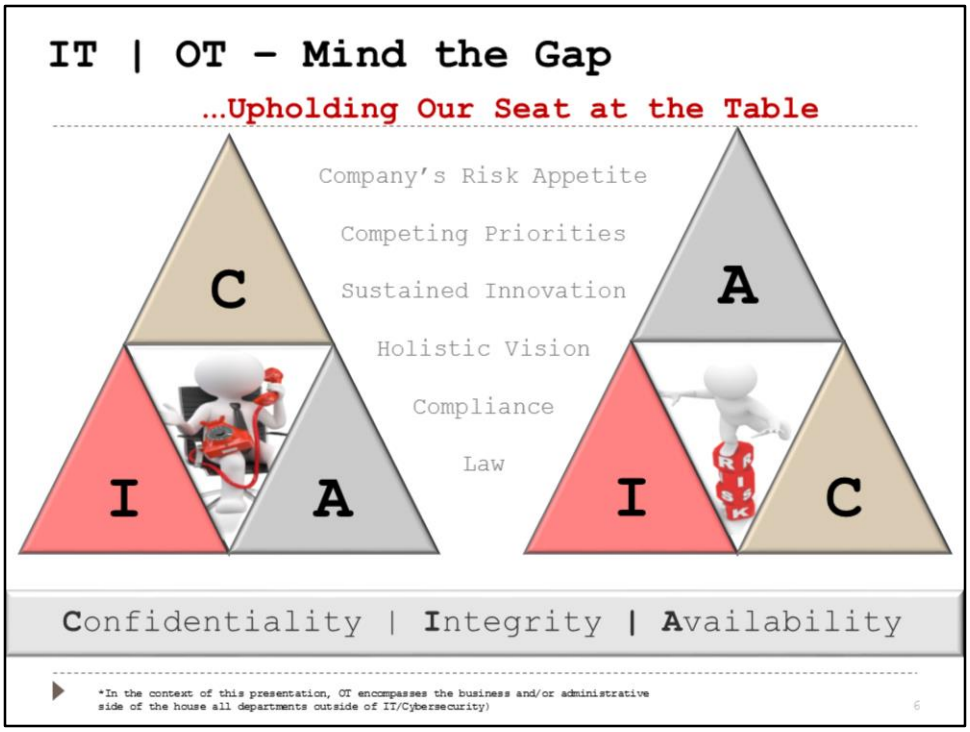
Finally…Cybersecurity gets a seat at the table!

The new trend is moving towards having an independent Cybersecurity department (outside of IT) that is challenged by a dynamic, persistent, proactively leveraging predictive analytics (Iot, artificial intelligence, machine learning) to identify, protect, detect, respond & recover (all in real time). In this ever interconnected world, Cybersecurity has become an integral function for just about every business activity. Cross-functional collaboration and adaptation of the proverbial interconnected reality warrants a shift in the way we approach Cybersecurity solutions.

A Few Examples Discussed:

SOC – White hat | Black Hat | Kinetic & Cyber layers
Traditional vs artificial intelligence, machine learning, dynamic, real-time, proactive
Operating System Agnostic Devices, Cloud hybrid environment, BYOD

*In the context of this presentation, OT encompasses the business and/or administrative side of the house (all departments outside of IT/Cybersecurity)



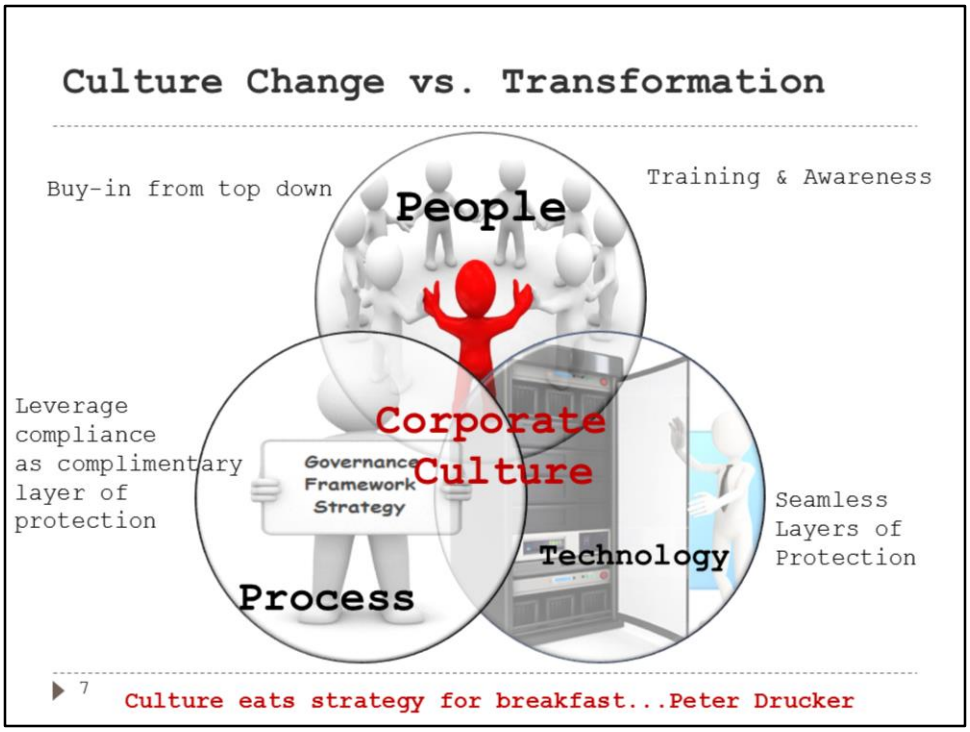
Discussion Summary – IT | OT – Mind The Gap!

*In the context of this presentation, OT encompasses the business and/or administrative side of the house (all departments outside of IT/Cybersecurity)

While it's great that in many environments, Cybersecurity finally has a seat at the table. Now we have the responsibility to keep that seat and continue to have a voice. More than ever, it's important to take a holistic view of the potential impact Cybersecurity services have on the business so we can be part of the solution and not be viewed as getting in the way of productivity

The CIA triad, which serves as a model that is diligently applied in the Cybersecurity landscape, is often the debate between IT and OT personnel given that operational functions mandate real-time expediency. We are often task with the challenge of supporting the business need to sustain innovation while ensuring the confidentiality and integrity of our systems/data.

Cybersecurity is no longer just about the technical skills, we need to know our company's risk appetite so we can align our strategy with the overall company's roadmap and be able to anticipate potential risks due to changes to the environment. We need to understand competing priorities so we can proactively determine how to manage limitation of resources

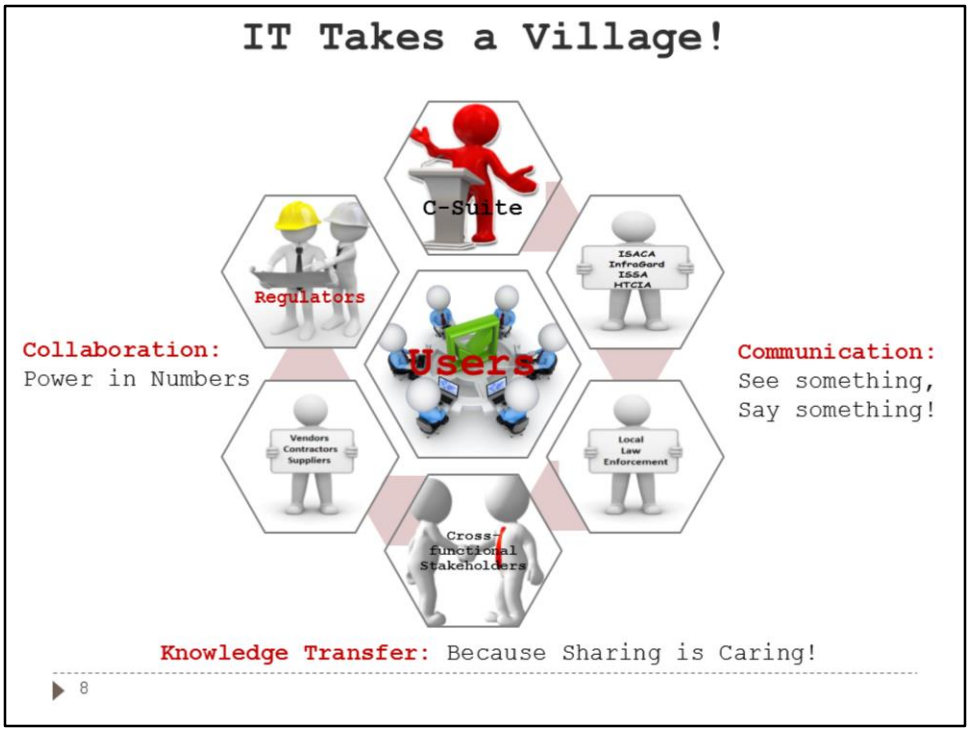


Discussion Summary – Culture Change vs. Transformation

Quote: Culture eats strategy for breakfast...Peter Drucker. We need to leverage the Cybersecurity foundation and build new layers that harness People, Process & Technology to introduce new methods of protection needed to address the digital age!

A Few Examples Discussed:

People: Need buy-in from top down | Need to ensure your Training & Awareness program aligns with your corporate culture.
Process: Compliance is NOT Cybersecurity but rather it should be a complimentary function that can be leveraged to further enhance your layers of protection. Cybersecurity Policies, Standards & Guidelines should align with the company's governance (not create unintended conflicts or contradictions). The Cybersecurity strategy should align with the company's vision, outlook and roadmap.
Technology: Leverage technology to continue building seamless layers of protection. Cybersecurity controls should be automated as much as possible in a way that they don't interfere with the business operations
Cybersecurity should never be part of the problem but rather enabling solutions!



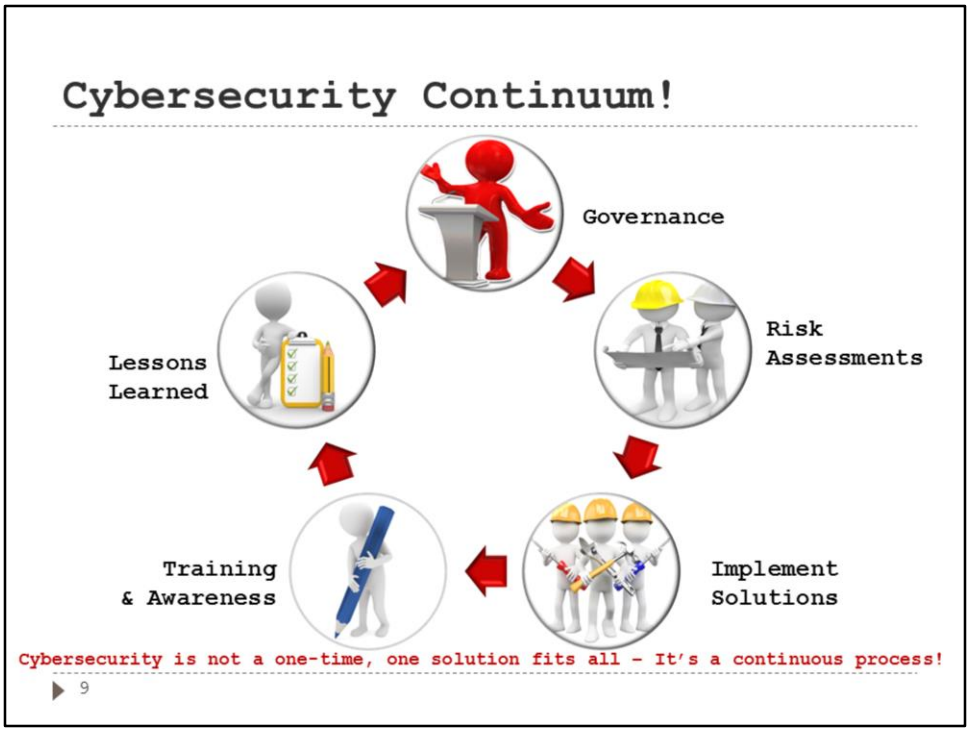
Discussion Summary – IT Takes a Village!

More than ever, collaboration, communication and knowledge transfer play a critical role in Cybersecurity. Not only do we have the challenge of keeping our seat at the table (play nice with others), but we have to keep up with the ever changing digital world. Securing devices becomes more difficult as we move from the physical world to virtual resources (such as the cloud). Not to mention that the bad guys tend to have an edge when it comes to levering cyberspace to conceal their traces and develop advanced attacks.

A Few Examples Discussed: We live in an interconnected world | There is NO one-way connection in cyberspace | Collaboration – Power in numbers | Communication (see something, say something) | Knowledge Transfer – Because sharing is caring!

Make sure you sustain buy-in from the top (not just your C-suite but your board of directors as well) | Leverage professional organizations such as ISACA, InfraGard, ISSA, HTCIA to stay up to date with the ever changing threat landscape | Get to know your local law enforcement (LLE). If you have critical infrastructure in your environment, it is very helpful if at least one person in your team has a clearance so you can get classified briefings
Make sure you include your remote sites for all Training & Awareness | Foster an environment of trust and collaboration with your vendors, contractors & suppliers.

Trust but verify…make sure you work closely with your Legal team to ensure contracts have the appropriate wording when it comes to Cybersecurity responsibilities, expectations and liabilities (in the event of a breach) | Keep in constant communication with your regulators so you understand how new regulations impact Cybersecurity solutions



Discussion Summary – Cybersecurity Continuum!

Cybersecurity is not a one-time, one solution fits all – It's a continuous process!

Review your Governance on regular intervals to ensure it is still relevant and in alignment with your company's strategic direction (which in some sectors can be very dynamic)
Perform both internal and external Risk Assessments
Leverage results of assessments to identify gaps, request needed resources and adjust your Cybersecurity strategy
Continue promoting cybersecurity awareness, We all play a key role when it comes to securing our assets
Document lessons learned and insure that you don't make the same mistakes twice

Questions?

Thank You!

Patricia Watson
@pmwatson