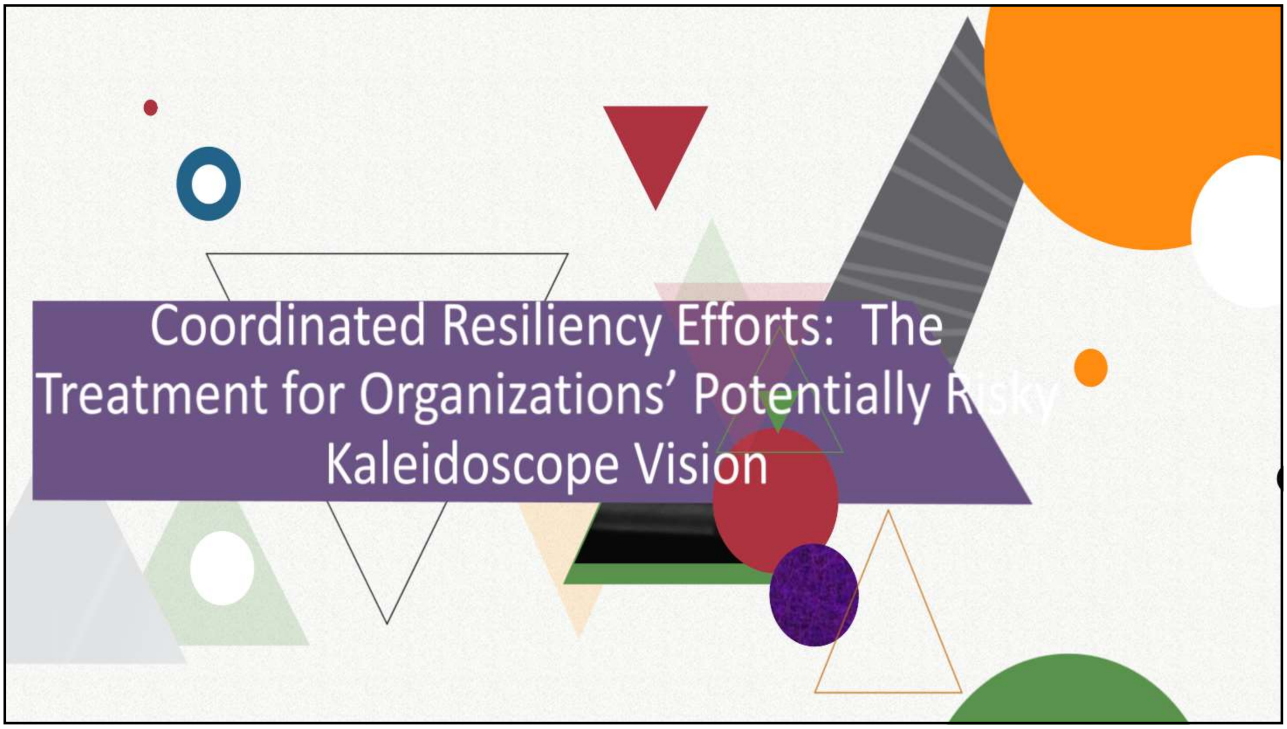
DRJ SPRING 2020
March 15-18, Orlando

Michele L. Turner
Head of Global Business Resiliency
Amazon

1

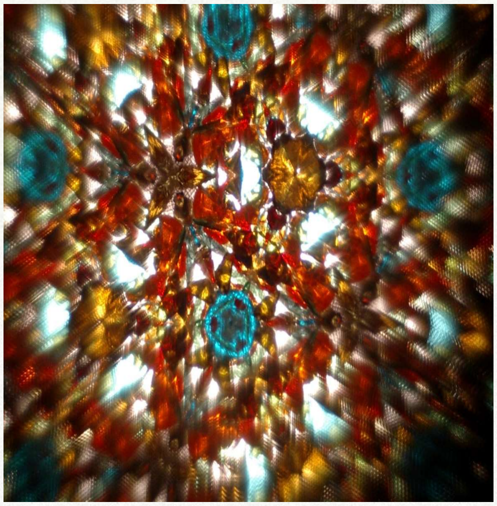


Coordinated Resiliency Efforts: The Treatment for Organizations' Potentially Risky Kaleidoscope Vision

2

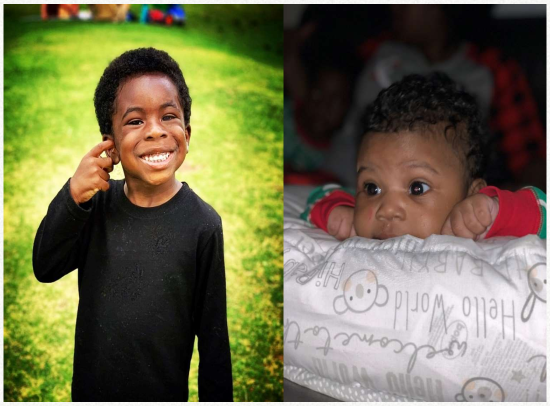
Agenda

- □**My Background**
- □***Level Set- Guidance***
  - □*Definitions*
  - □*Guiding Principles*
- □***Opportunities and Challenges- Causes, Symptoms, and Results***
  - □ *Threats and Vulnerabilities*
  - □*Resulting Risks*
- □***Potential Mitigations- Potential Treatment***
  - □*Cross Walk Connections*
- □***Key Takeaways- Vision Clarity***

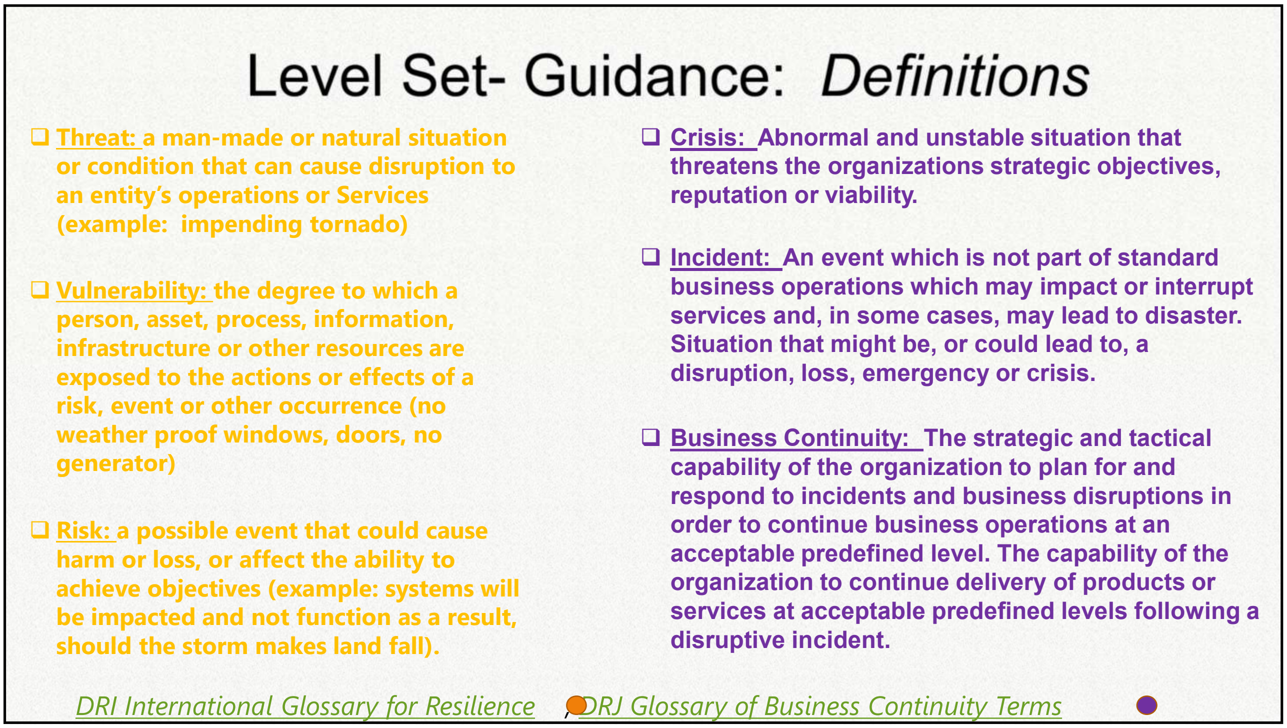


My Background

- □26+ years in the Business Continuity Industry
  - □Masters of Science in Business Continuity- Norwich University
- □Subject Matter Expertise in Governance, Risk, Compliance and Controls
  - □Technology, Financial, E-Commerce, Consulting Industries
- □ Engaged with DRJ for 15+ years
  - □ Editorial Advisory Board, Generally Accepted Practices Committee



- □And…I'M A GRANDMA!!!!

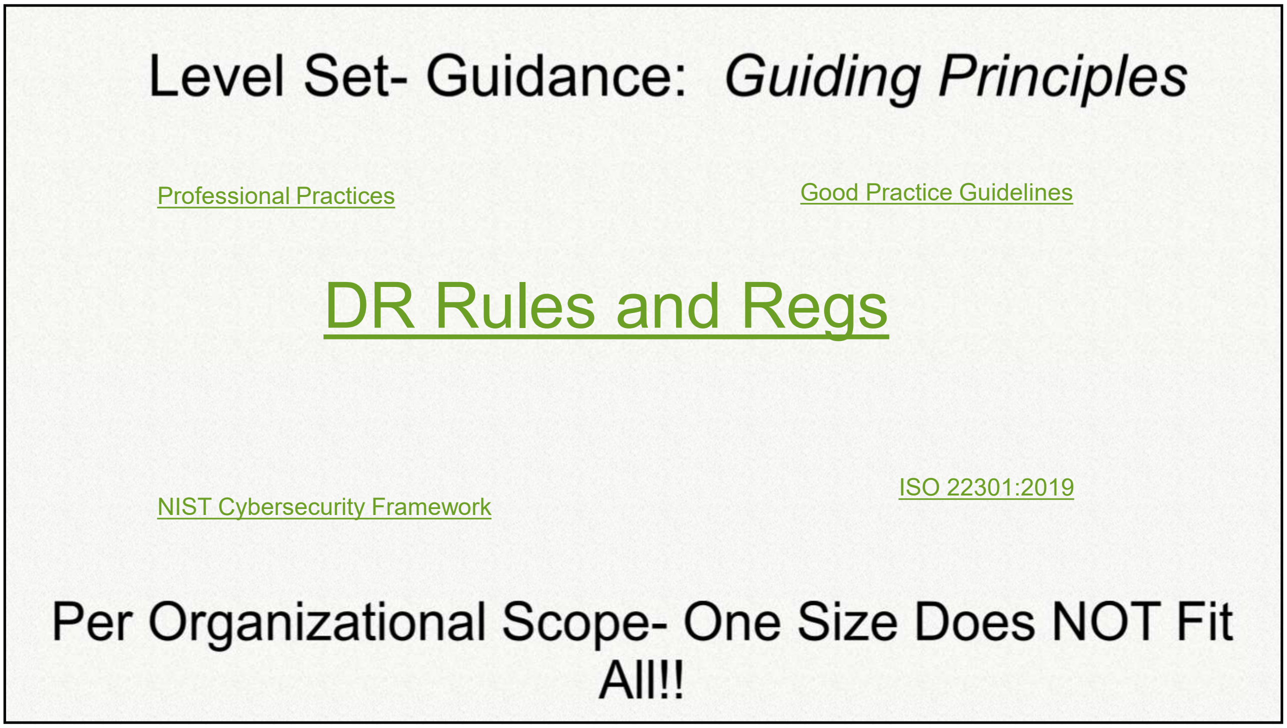


Level Set- Guidance: *Definitions*

- □ Threat: a man-made or natural situation or condition that can cause disruption to an entity's operations or Services (example: impending tornado)
- □ Vulnerability: the degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence (no weather proof windows, doors, no generator)
- □ Risk: a possible event that could cause harm or loss, or affect the ability to achieve objectives (example: systems will be impacted and not function as a result, should the storm makes land fall).
- □ Crisis: Abnormal and unstable situation that threatens the organizations strategic objectives, reputation or viability.
- □ Incident: An event which is not part of standard business operations which may impact or interrupt services and, in some cases, may lead to disaster. Situation that might be, or could lead to, a disruption, loss, emergency or crisis.
- □ Business Continuity: The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level. The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

DRI International Glossary for Resilience ●, *DRJ Glossary of Business Continuity Terms* ●

5



Level Set- Guidance: *Guiding Principles*

Professional Practices

Good Practice Guidelines

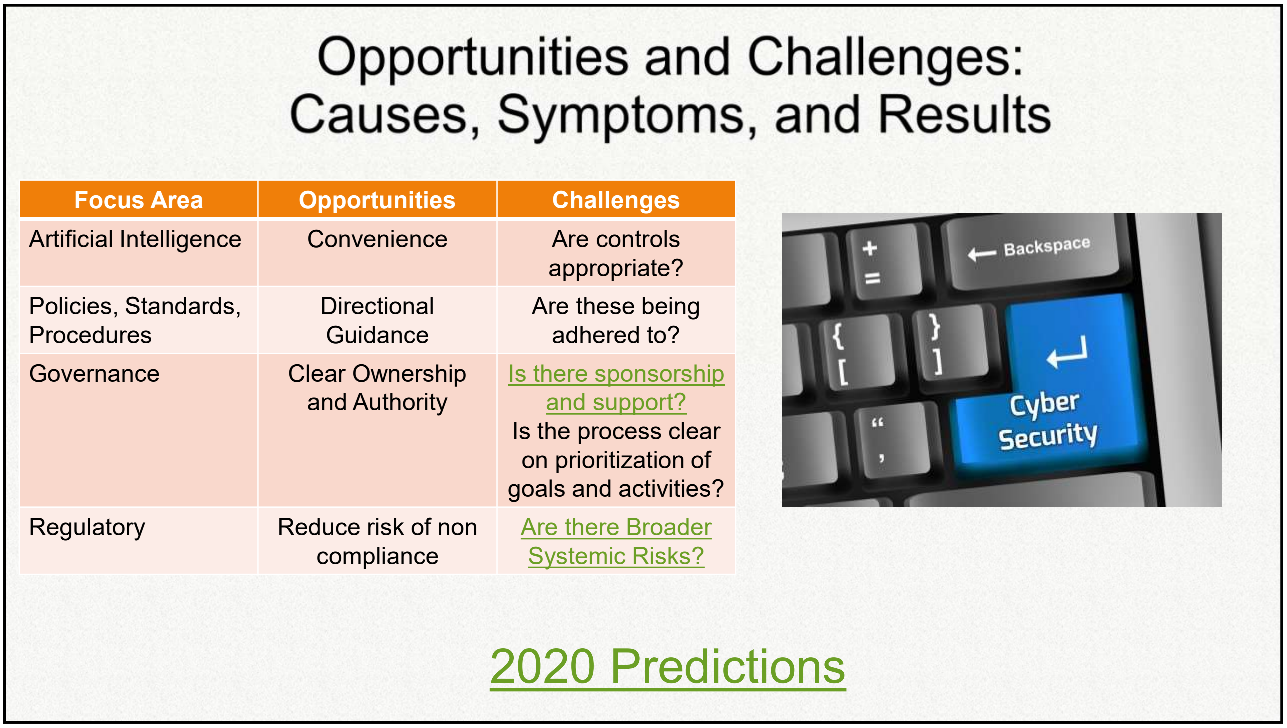
DR Rules and Regs

NIST Cybersecurity Framework

ISO 22301:2019

Per Organizational Scope- One Size Does NOT Fit All!!

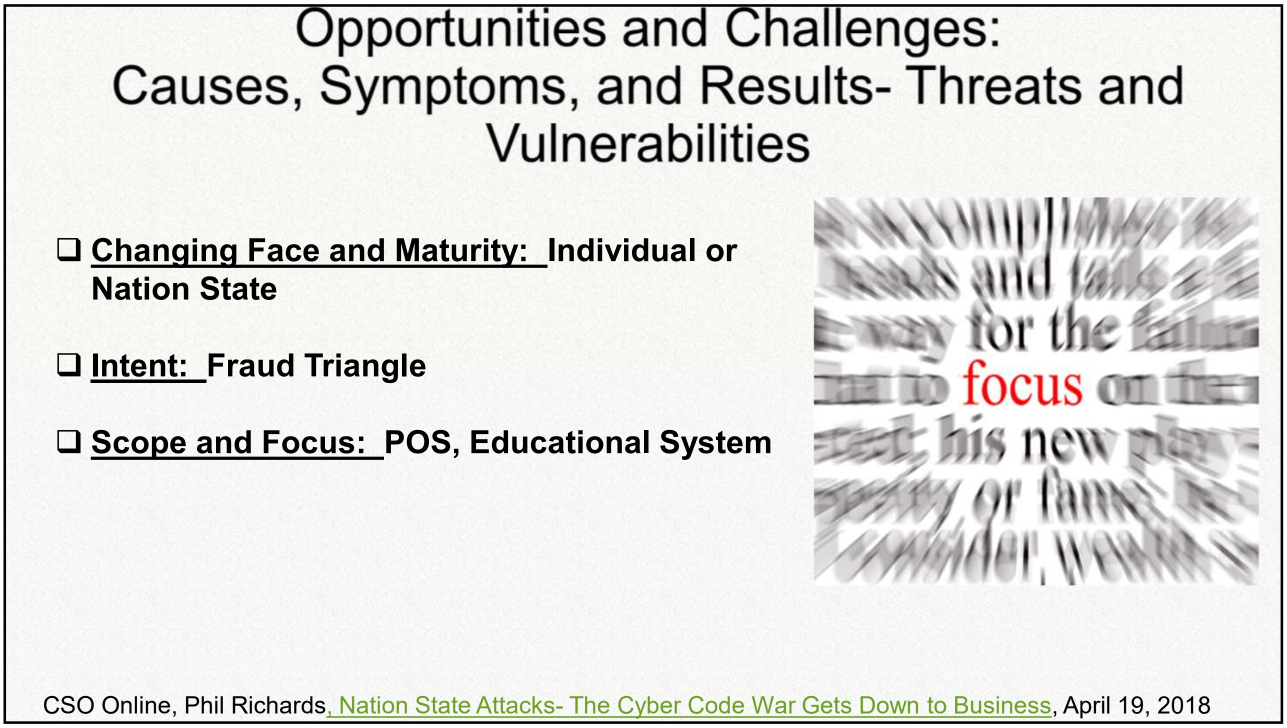
6



Opportunities and Challenges: Causes, Symptoms, and Results

Focus Area	Opportunities	Challenges
Artificial Intelligence	Convenience	Are controls appropriate?
Policies, Standards, Procedures	Directional Guidance	Are these being adhered to?
Governance	Clear Ownership and Authority	Is there sponsorship and support? Is the process clear on prioritization of goals and activities?
Regulatory	Reduce risk of non compliance	Are there Broader Systemic Risks?

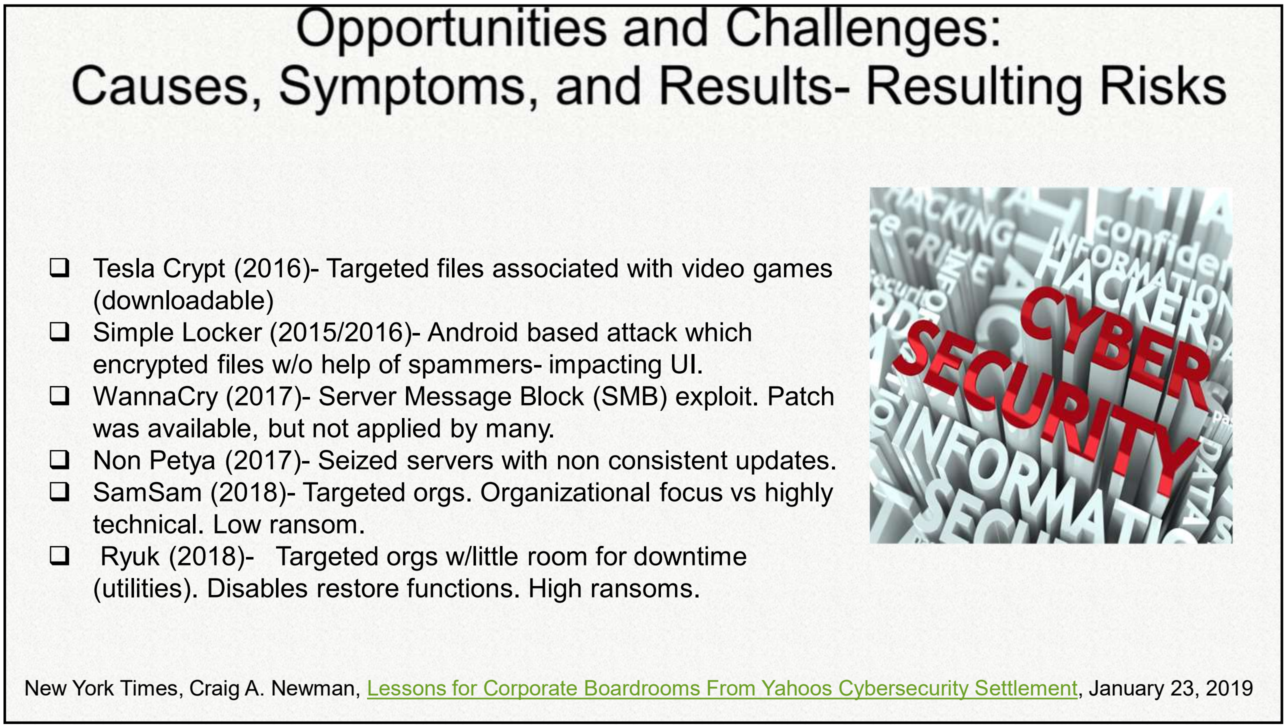
2020 Predictions



Opportunities and Challenges: Causes, Symptoms, and Results- Threats and Vulnerabilities

- ❑ **Changing Face and Maturity: Individual or Nation State**
- ❑ **Intent: Fraud Triangle**
- ❑ **Scope and Focus: POS, Educational System**

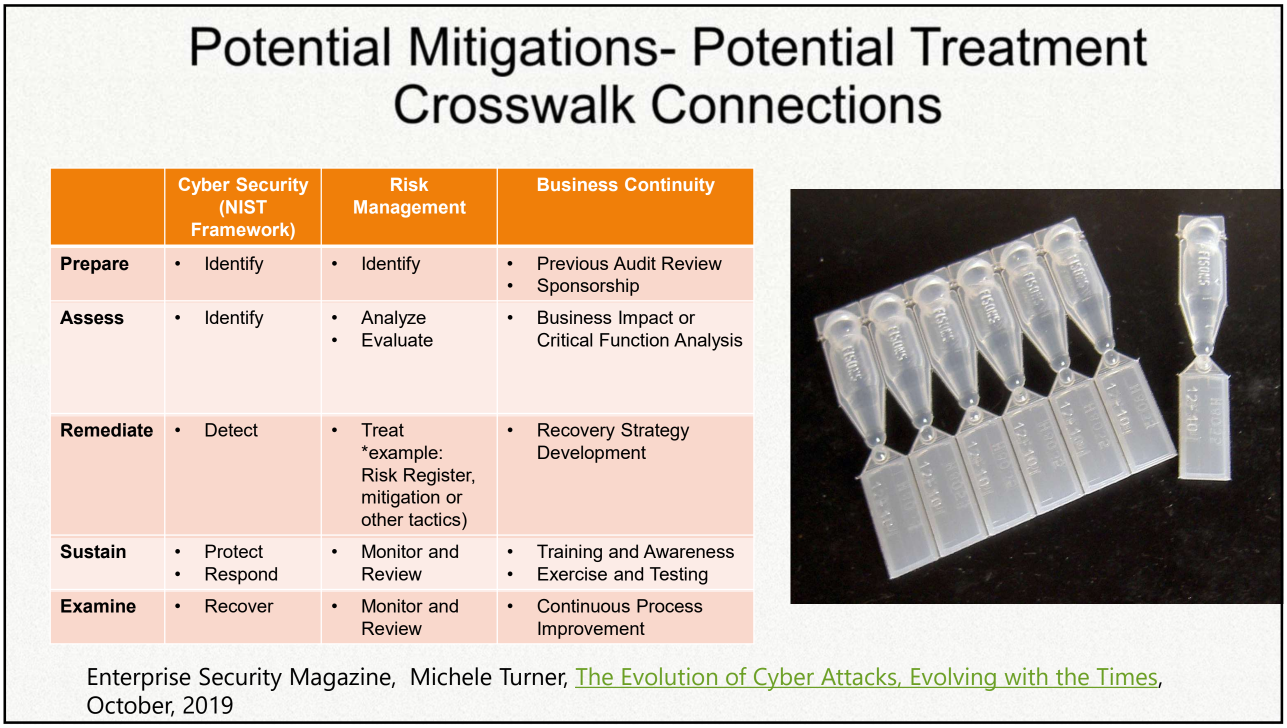
CSO Online, Phil Richards, Nation State Attacks- The Cyber Code War Gets Down to Business, April 19, 2018



Opportunities and Challenges: Causes, Symptoms, and Results- Resulting Risks

- ❑ Tesla Crypt (2016)- Targeted files associated with video games (downloadable)
- ❑ Simple Locker (2015/2016)- Android based attack which encrypted files w/o help of spammers- impacting UI.
- ❑ WannaCry (2017)- Server Message Block (SMB) exploit. Patch was available, but not applied by many.
- ❑ Non Petya (2017)- Seized servers with non consistent updates.
- ❑ SamSam (2018)- Targeted orgs. Organizational focus vs highly technical. Low ransom.
- ❑ Ryuk (2018)- Targeted orgs w/little room for downtime (utilities). Disables restore functions. High ransoms.

New York Times, Craig A. Newman, Lessons for Corporate Boardrooms From Yahoos Cybersecurity Settlement, January 23, 2019



Potential Mitigations- Potential Treatment Crosswalk Connections

	Cyber Security (NIST Framework)	Risk Management	Business Continuity
Prepare	• Identify	• Identify	• Previous Audit Review • Sponsorship
Assess	• Identify	• Analyze • Evaluate	• Business Impact or Critical Function Analysis
Remediate	• Detect	• Treat *example: Risk Register, mitigation or other tactics)	• Recovery Strategy Development
Sustain	• Protect • Respond	• Monitor and Review	• Training and Awareness • Exercise and Testing
Examine	• Recover	• Monitor and Review	• Continuous Process Improvement

Enterprise Security Magazine, Michele Turner, The Evolution of Cyber Attacks, Evolving with the Times, October, 2019

Key Takeaways- Vision Clarity

- ❑ Common Understanding of Challenge, Threats and Vulnerabilities
- ❑ Understand Potential Approaches
- ❑ Engage Appropriate Stakeholders
- ❑ Leverage, Leverage, Leverage
- ❑ Communicate, Communicate, Communicate
- ❑ Pivot with the Times

11

DRJ SPRING 2020
March 15-18, Orlando

Thank You!!

mlturner@amazon.com

12