

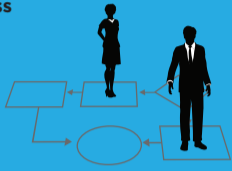













Enterprise Information Security

FUTURE-PROOFING PROCESSES

RECOMMENDATION	ACTIONS	RESULTS
 <p>Shift Focus from Technical Assets to Critical Business Processes</p>	<ul style="list-style-type: none"> - Acquire deep understanding of business processes from end-to-end - Work with the business to document business processes 	<ul style="list-style-type: none"> - Discern “normal” from “abnormal” conditions within a business process - Ascertain how attackers would undermine processes - Make security controls more effective to better protect the business 
 <p>Institute Business Estimates of Cyber-Security Risks</p>	<ul style="list-style-type: none"> - Articulate cybersecurity risks in business terms - Define scenarios describing the likelihood of incidents and magnitude of business impact - Hone risk quantification techniques to approximate projected monetary losses <p>\$100,000? \$1 Million? \$10 Million? \$100 Million?</p>	<ul style="list-style-type: none"> - Weigh cybersecurity risks vs. business rewards - Prioritize cybersecurity risks against other risks - Conduct business risk conversations on materiality of risks and adequacy of mitigation strategies 
 <p>Establish Business-Centric Risk Assessments</p> 	<ul style="list-style-type: none"> - Implement a more automated risk-assessment process - Track risks as they are identified, evaluated, accepted, and remediated - Modify risk-acceptance process to enable increased risk for select projects short-term 	<ul style="list-style-type: none"> - Realize a holistic view of cybersecurity risks - Make it workable to hold the business accountable for managing risks - Take advantage of time-sensitive business opportunities 
<p>Set a Course for Evidence-Based Controls Assurance</p> 	<ul style="list-style-type: none"> - Establish procedures to systematically collect evidence and report on the efficacy of security controls - Document and review controls, focusing on the most critical - Automate collection and reporting over time 	<ul style="list-style-type: none"> - Optimize security controls - Enable efficient audits that are not disruptive to the business - Improve internal and 3rd-party assessments 
<p>Develop Informed Data-Collection Methods</p> 	<ul style="list-style-type: none"> - Examine the types of security questions data analytics can answer - Build a set of data-analytics use cases, following an iterative process - Enrich analysis with business process data and external threat intelligence 	<ul style="list-style-type: none"> - Identify relevant sources of data and know how to gain access to this data - Obtain meaningful analysis - Make progress towards a data-analytics capability 