



CYBERSECURITY: What Should Companies Be Doing to Prepare

Year-End CPE Program
Denver
December 7, 2016

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.



**WITH YOU
TODAY**



MAURICE LIDDELL
Managing Director
BDO Consulting

+1 713-407-3265
mliddell@bdo.com

AGENDA

- ▶ Today's Threat Landscape
- ▶ Cybersecurity Risk Management Overview
- ▶ Understanding Your Risk
- ▶ Regulatory Requirements
- ▶ Cybersecurity Mitigation
- ▶ Conclusion

TODAY'S THREAT LANDSCAPE

CYBERSECURITY TODAY



TODAY'S THREAT LANDSCAPE

INTERNAL THREAT: Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

COMPUTER INTRUSIONS:
This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was \$4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of \$13.1 million.

BUSINESS E-MAIL COMPROMISE: Between January 2015 and June 2016, there has been a 1,300% increase in identified exposed losses, a combined exposed dollar loss of more than \$3 billion.

RANSOMWARE: Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack.

- Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
- 2016 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016
- FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA
- Understanding the Depth of the Global Ransomware Problem, Osterman Research Survey Report, Published August 2016, Sponsored by Malwarebytes

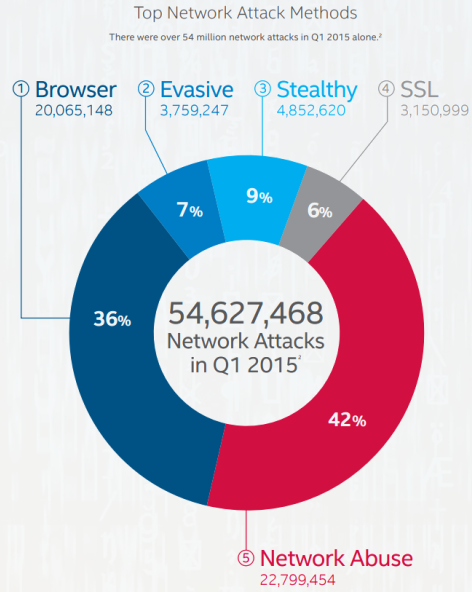
CYBERSECURITY TODAY



TODAY'S THREAT LANDSCAPE

What Data Are They Taking?

Data types	Internal Actors	External Actors
Customer Information	27%	32%
Employee Information	33%	28%
Intellectual Property	15%	14%
Payment Card Information	11%	15%
Other Financial Information	14%	11%



- Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
- Intel Security Report, Dissecting the Top Five Network Attack Methods: A Thief's Perspective



TODAY'S LANDSCAPE: DATA BREACHES BY THE NUMBERS



TODAY'S THREAT LANDSCAPE

48%
caused by malicious or criminal attacks

\$4 million
average cost of a data breach

29%
increase in total cost of data breach since 2013

\$158
average cost per lost or stolen record

\$355
average cost per lost or stolen record in healthcare organizations

LATEST TACTIC FOR DELIVERING RANSOMWARE



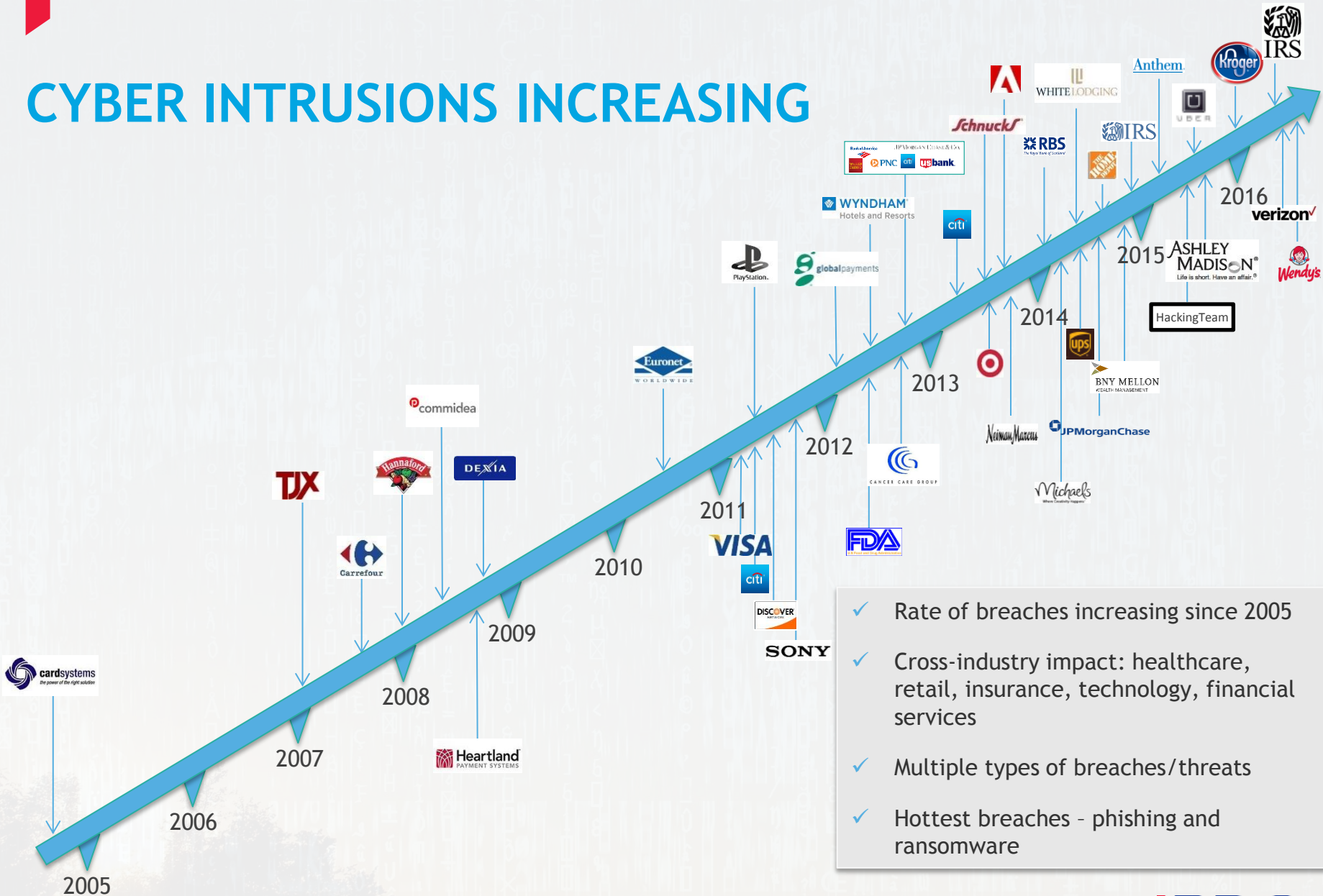
TODAY'S THREAT LANDSCAPE

Windows Script Files (WSF)

- ▶ Allow a **variety of scripting languages** to mix within a single file
- ▶ **Not automatically blocked** by some email clients
- ▶ Number of *blocked* emails containing malicious WSF has gone from **22,000** in June to **2.2 million** in September
- ▶ Commonly deployed via **travel-related emails**, tricking individuals into installing ransomware

The estimated cost of ransomware attacks is going to total
\$1 billion in 2016

CYBER INTRUSIONS INCREASING



- ✓ Rate of breaches increasing since 2005
- ✓ Cross-industry impact: healthcare, retail, insurance, technology, financial services
- ✓ Multiple types of breaches/threats
- ✓ Hottest breaches - phishing and ransomware



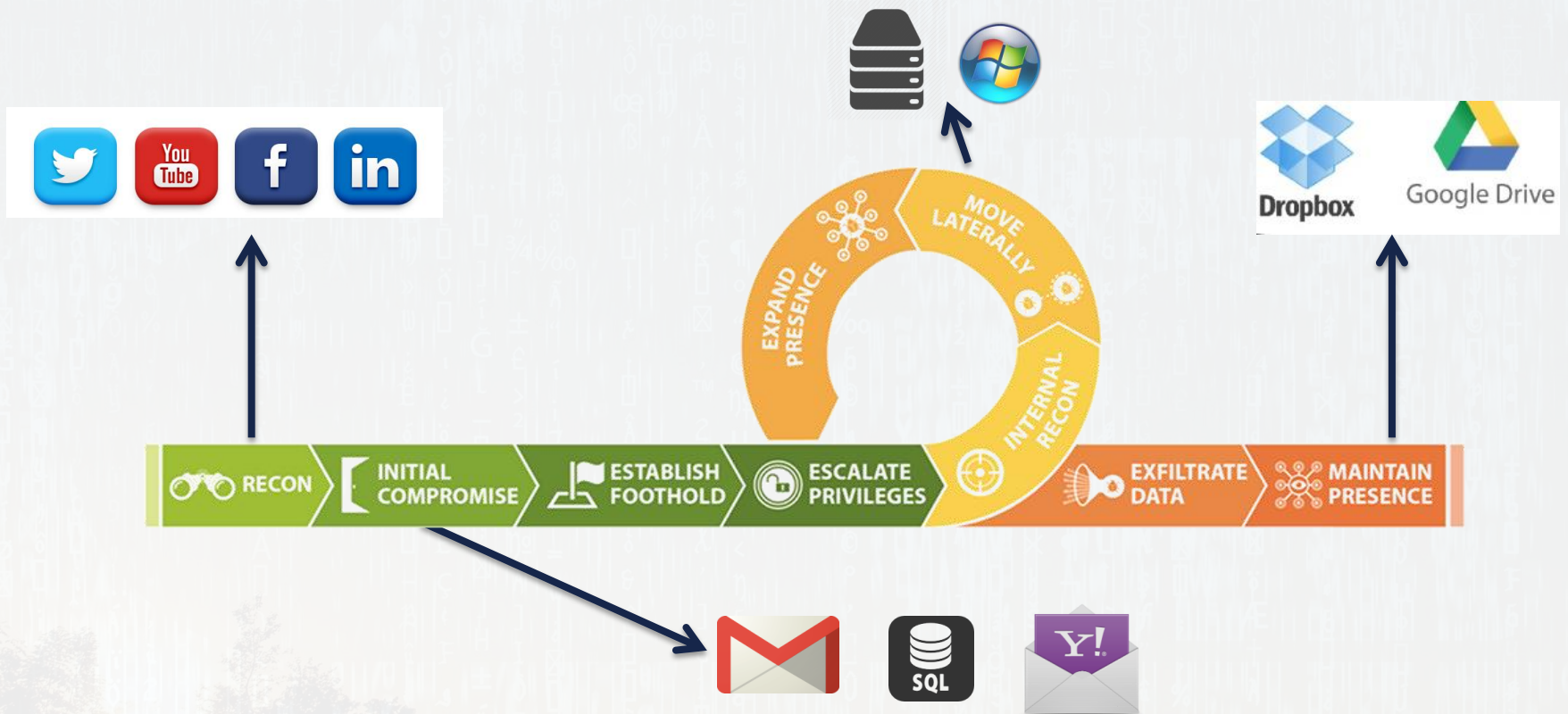
TODAY'S THREAT LANDSCAPE

CYBER THREATS CANNOT BE ELIMINATED, THEY CAN ONLY BE MITIGATED

“I always tell [our workers], ‘Don't ever forget that at the end, we're dealing with **a choice that some human made** on a keyboard somewhere else in the world ... There was **a man or woman on the other end of this.**’” - *Admiral Michael Rogers, Director, NSA and Cyber Command*

“The Russians **hack our systems** all the time, not just government, but also corporate and personal systems. And so do the Chinese and others, including non-state actors. The point is, **cyber will continue to be a huge problem** for the next Presidential administration, as it has been a challenge for this one.” - *Hon. James R. Clapper, Director of National Intelligence*

ANATOMY OF A HACK





CYBERSECURITY RISK MANAGEMENT OVERVIEW

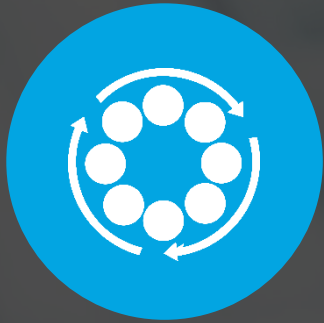




CYBERSECURITY RISK MANAGEMENT OVERVIEW

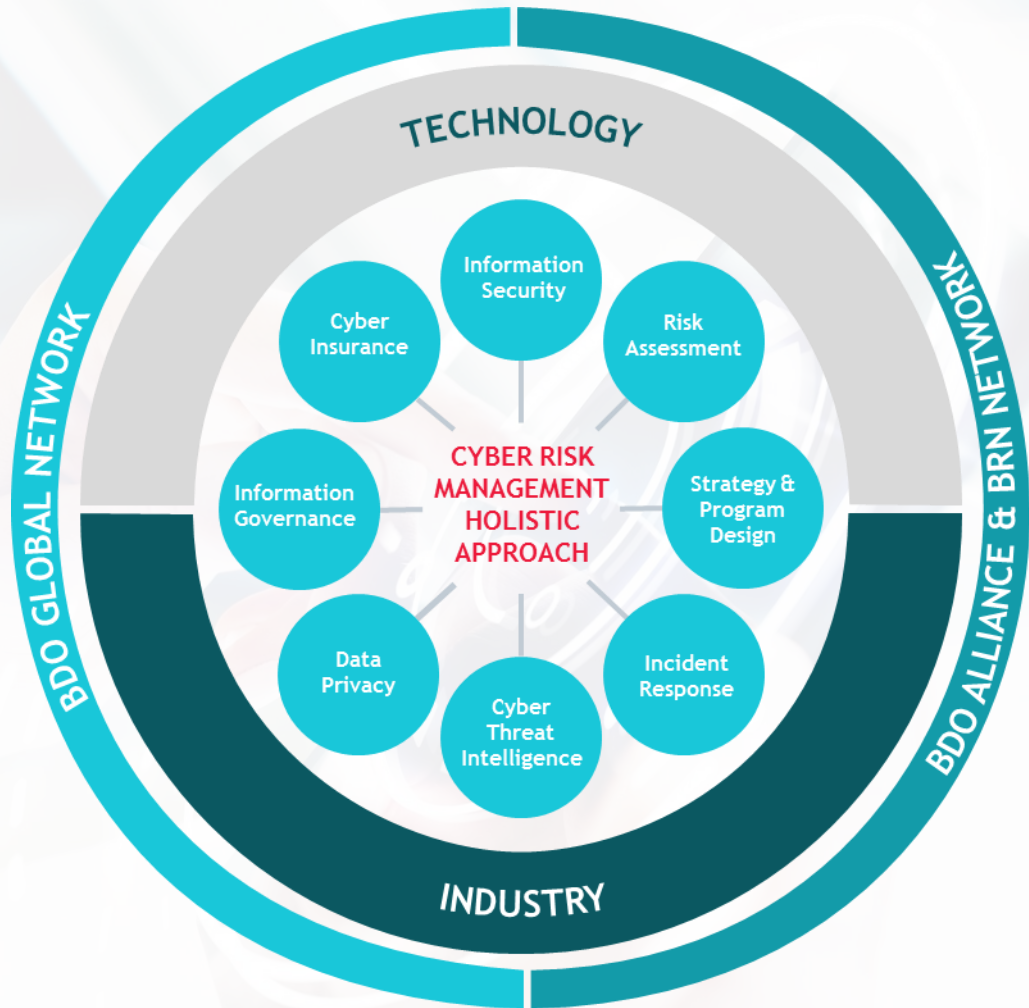
WHAT IS “CYBERSECURITY RISK MANAGEMENT PROGRAM”?

- ▶ **Integrated** set of policies, processes, technologies and controls that minimize vulnerabilities and protect against threat to support
- ▶ **Confidentiality** - information kept private and secure
- ▶ **Integrity** - data not inappropriately modified, deleted or added
- ▶ **Availability** - systems/information available to whom requires them



CYBERSECURITY RISK MANAGEMENT OVERVIEW

A HOLISTIC APPROACH





UNDERSTANDING YOUR RISK



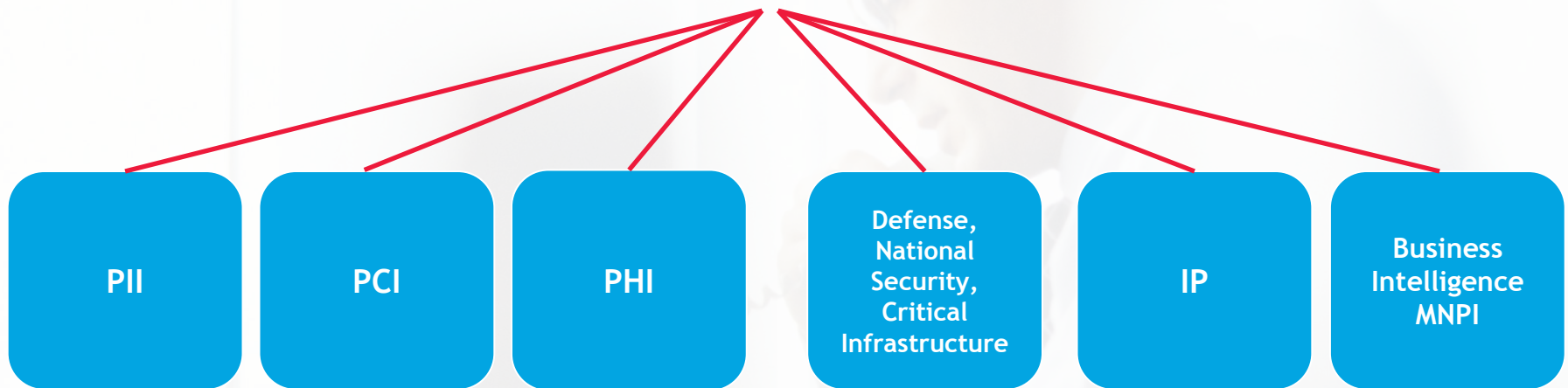
UNDERSTANDING YOUR RISK



THREAT
VULNERABILITY
+ CONSEQUENCE

RISK

TARGETED DATA





UNDERSTANDING YOUR RISK

CYBERSECURITY RISKS

A set of scenarios based on impacts to **Assets** by potential **Threats** and their ability to leverage **Vulnerabilities**



ASSETS

Processes, Information, and Systems with varying degrees of value to the organization



THREATS

Actors that are motivated to attack or misuse your assets



VULNERABILITIES

Flaws, control weaknesses or exposures of an asset to compromise



UNDERSTANDING YOUR RISK

DIGITAL ASSET VALUATION

Three Principles of Digital Asset Valuation

1. Consider **who gets value** from the asset
2. Understand the role your digital assets play in **creating economic value / generating revenue**
3. **Look forward** - valuing your digital assets requires an outward view (previously invested costs to create the asset are “sunk”)

Understanding the Value of Digital Assets

- ▶ **Intrinsic** - Critical element that allows the digital asset to exist in the first place (e.g. the person, binary data, physical object, legal contract etc.)
- ▶ **Extrinsic** - Opportunities to leverage the digital asset making it more useful to prospective users
- ▶ **Sum it up** - Metadata defines the extrinsic value of your digital assets, informing their value



UNDERSTANDING YOUR RISK

DATA CLASSIFICATION

- ▶ Review and analyze report(s)
- ▶ Readjust framework and re-classify data as needed

Act

- ▶ Data assets
- ▶ Data custodians

Identify

DATA CLASSIFICATION

Classify

Plan

- ▶ Create classification framework
- ▶ Develop protection profiles









UNDERSTANDING YOUR RISK

LIFE CYCLE OF DATA PRIVACY AND PROTECTION



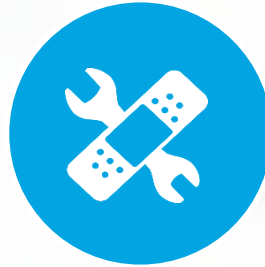
MOTIVATIONS AND INCENTIVES

	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



UNDERSTANDING YOUR RISK

VULNERABILITIES



SOFTWARE PATCHING

Lack of software updates



ACCESS CONTROL

Who has access to your system and do they really need it?



THIRD PARTY VENDORS

Are your third party vendors secure?



PEOPLE

Internal actors up to no good or being exploited



REGULATORY REQUIREMENTS



REGULATORY REQUIREMENTS

PROPOSED NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES REGULATION

- ▶ In September 2016, Gov. Andrew Cuomo announced the proposal of a new first-in-the-nation regulation
- ▶ The regulation would require banks, insurance companies, and other financial services institutions regulated by the NYSDF to establish and maintain a cybersecurity program
- ▶ The program would include the need for:
 - A written cybersecurity policy
 - Designation of a CISO
 - Implementation of policies and procedures designed to ensure security



REGULATORY REQUIREMENTS

EXISTING AND FORTHCOMING GUIDANCE

- ▶ Presidential Policy Directive (PPD) on Cyber Incident Coordination
- ▶ FinCen FAQs on Customer Due Diligence Requirements for Financial Institutions
- ▶ *Proposed Cybersecurity Disclosure Act of 2015*
- ▶ BDO along with the other Big 8 Audit Firms have been working with AICPA as part of the ASEC Cybersecurity Working Group to develop the Cybersecurity Attestation Guideline which will establish a new audit service in the market place.



CYBERSECURITY MITIGATION

BDO CYBERSECURITY FRAMEWORK

Key Policy & Process Domains

- ▶ Data privacy / protection
- ▶ Identity & access management
- ▶ Threat & risk intelligence
- ▶ Third party / vendor management
- ▶ Incident response & planning
- ▶ Asset inventories
- ▶ Metrics / reporting
- ▶ Training / awareness

Cybersecurity Lifecycle



Governance & Strategy

- ▶ Cybersecurity risk profile management
- ▶ Cybersecurity risk management program
- ▶ Organization roles and responsibilities (Board of Directors, Executive Management, etc.)
- ▶ Investment optimization
- ▶ Legal & compliance
- ▶ Cyber insurance



CYBERSECURITY MITIGATION

RECOMMENDED STEPS FOR MITIGATION



**AWARENESS AND
TRAINING**



CONFIGURATION



SPAM FILTERS



MACRO SCRIPTS



E-MAIL DETECTION



**SOFTWARE RESTRICTION
POLICIES**



**ANTI-VIRUS and
MALWARE**



APP WHITELISTING



ACCESS CONTROLS



CATEGORIZE DATA



CYBERSECURITY MITIGATION

RECOMMENDED STEPS FOR REMEDiation



ISOLATE

Affected computers



DO NOT CLEAN OR RE-IMAGE

Affected computers



CONTACT LAW ENFORCEMENT

Provide relevant logs



IMPLEMENT

Incident Response and BC Plans



CYBERSECURITY MITIGATION

THREAT INTELLIGENCE



Private Sector
Threat
Information



Government Classified
and Unclassified
Evidence and
Intelligence



Cyber Threat
Intelligence

INFORMATION SHARING CHANNELS



CYBERSECURITY MITIGATION





CONCLUSION

SPEAKER BIO



MAURICE LIDDELL

Managing Director
BDO Consulting

Direct: +1 713-407-3265
mliddell@bdo.com

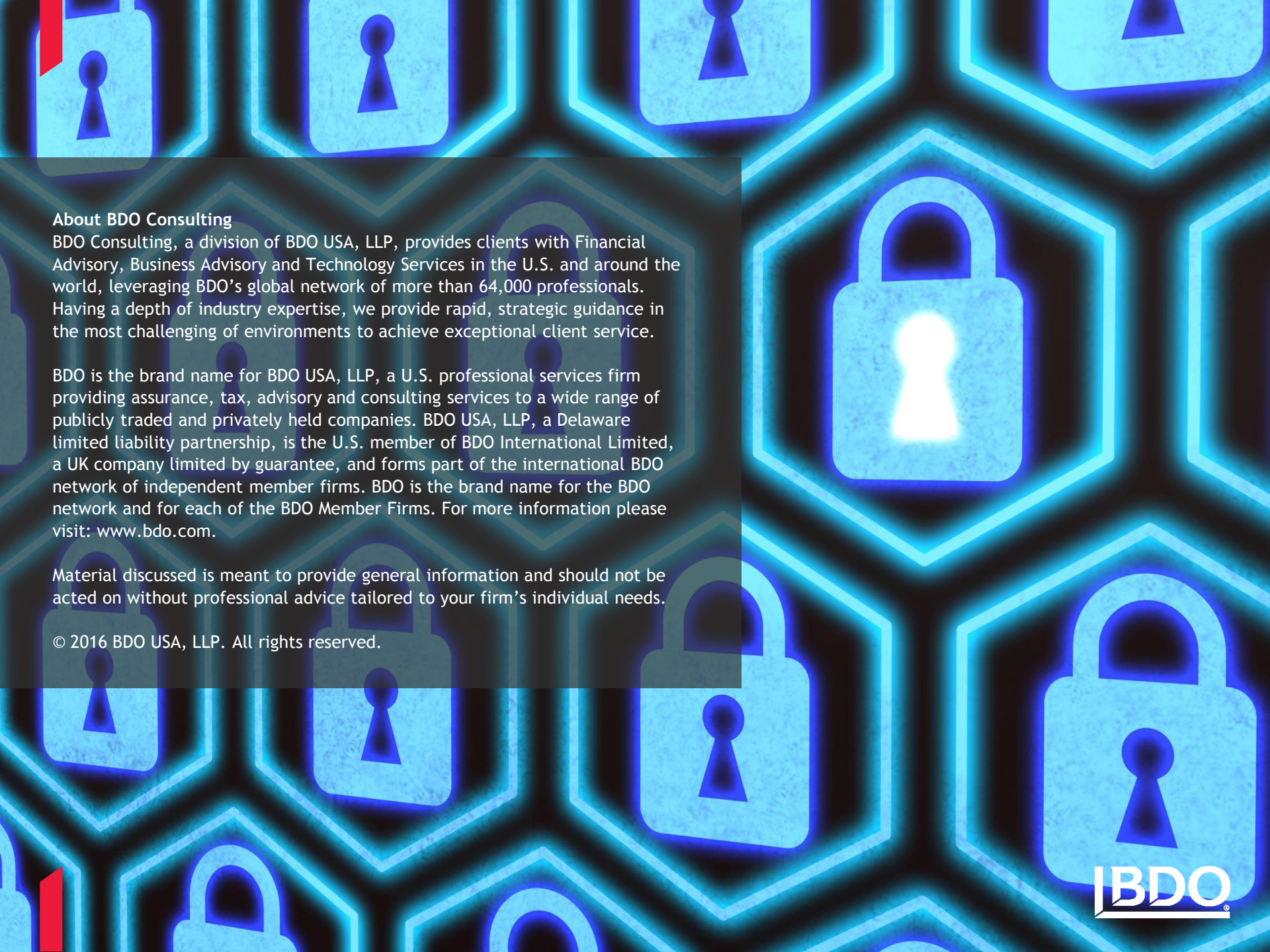
Maurice Liddell is a Managing Director in the Technology Advisory Services practice. With a spectrum of insights gained from the world's largest IT consulting firm, to hands-on experience as an engineer, Maurice uses his technology background to design and implement successful technology solutions to improve business operations and manage technology related risks for clients.

His track record includes responsibility for \$25 million budget programs; reduction of IT operating costs from \$22 million to \$13.5 million; transforming IT of the largest private school system in the U.S. to deliver greater value to shareholders; serving as chief technologist for the planning and launch of a B2B exchange; running global IT operations for a Fortune 500 company; managing SOX and Technology Risk Management programs; evaluating and preparing organizations to comply with regulatory (e.g., HIPAA, HITECH, PCI, etc.) and industry (e.g., ISO 27002) security standards, performing Business Impact Assessments (BIA) and developing Business Continuity Plans (BCP) and the successful management of full cycle projects ranging from custom software development to ERP implementations to enterprise infrastructure solutions.



OUR CYBERSECURITY SERVICES

- ▶ Cyber Risk Management Strategy & Program Design
- ▶ Cyber Risk Assessment & Security Testing
- ▶ Data Privacy & Protection
- ▶ Security Architecture & Transformation
- ▶ Incident Response Planning
- ▶ Business Continuity Planning & Disaster Recovery
- ▶ Digital Forensics & Cyber Investigations
- ▶ Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation



About BDO Consulting

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO's global network of more than 64,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

© 2016 BDO USA, LLP. All rights reserved.