DORSEY™
always ahead

Energy Industry Group Webinar

How to Prepare for Cybersecurity Threats

January 19, 2016

Bob Cattanach, Dorsey & Whitney LLP
Michael Gomez, KPMG LLP
Ronald Plesco, KPMG LLP

DORSEY™
always ahead

Energy Industry Group Webinar

How to Prepare for Cybersecurity Threats

Contents

Speaker Biography's
Bob Cattanach, Dorsey & Whitney LLP
Michael Gomez, KPMG LLP
Ron Plesco, KPMG LLP

PowerPoint Slides prepared by Bob Cattanach, Dorsey & Whitney LLP

Connecting the dots: A proactive approach to cybersecurity oversight in the boardroom, Ron Plesco and Michael Gomez, KPMG LLP (December 2015)

Dorsey Partner Bob Cattanach Discusses Cybersecurity in: ***Paris Attacks Show the Good and Bad of High-Tech Revolution***, Matthew Schofield, McClatchy DC (November 20, 2015)
Available on Dorsey.com: http://www.mcclatchydc.com/news/nation-world/world/article45621927.html

So, Who Owns Your Energy-Use Data?, Joe Hall, Bob Cattanach and Brad Hammer, WindPower Engineering and Development (October 2015)
Available on Dorsey.com:
http://issuu.com/wtwhmedia/docs/windpower_oct_digital_issue_vs1/41?e=7799406/30659156

vUpdate Video: ***Five Steps to Prepare for a Data Breach***, Bob Cattanach, Dorsey & Whitney LLP (August 10, 2015)
Available on Dorsey.com: https://www.dorsey.com/newsresources/publications/client-alerts/2015/08/five-steps-to-prepare-for-a-data-breach

10 Common Cyber Incident Response Mistakes: Does your incident response program solve or exacerbate your security problems?
Forensic Focus, KPMG LLP, December 2014

PEOPLE

Robert E. Cattanach

Partner

cattanach.robert@dorsey.com

Overview

BOB HELPS CLIENTS NAVIGATE THE COMPLEXITIES OF REGULATORY LAW, ESPECIALLY IN THE AREA OF CYBERSECURITY AND COMPLIANCE, AND PROVIDES THE PERSPECTIVE AND SKILLS OF A SEASONED TRIAL LAWYER TO PROTECT THEIR INTERESTS IN THE COURTROOM.

His technical background enables him to understand the complex business challenges associated with today’s cyber world, and provide the strategic acumen to achieve success.

Bob’s decades of experience as a trial lawyer also enable his clients to achieve their business objectives if other means of resolution cannot be achieved. Bob has an active trial docket in courts around the country, where his innovative thinking, collaborative client approach, and keen strategic insights have provided his clients with a long string of successful verdicts and appeals. Under Bob’s leadership, Dorsey teams have helped our clients achieve precedent-setting results, especially in the complex area of constitutional challenges to government overreach.

Experience

Bob has represented numerous clients in breach responses, development of privacy policies and procedures, and provided counsel to corporate Boards of Directors, and Audit Committees on matters of cybersecurity, privacy and internal governance. Bob’s long history of interaction with key government agencies began with his service of the United States Department of Justice, Civil Division, which represents the interests of the United States and its agencies, including the CIA, FBI, Departments of State, Defense and Energy. His longstanding relationship with those agencies enables him to engage with key players on major cyber issues, and be the “go-to” attorney for all matters cyber.

Bob is also a much-sought-after commentator and contributor to professional and journalistic coverage of cybersecurity issues, ranging from the New York Times and USA Today to numerous television media and the Sedona Conference Working Group 11 on cyber matters.

Professional & Civic

Professional Achievements

- The Sedona Conference Working Group on Data Security and Privacy Liability, Working Group 11 (June 2015)
- The Sedona Conference All Voices Meeting (2014)
- Chairman of the Board, Ordway Center for the Performing Arts
- Co-Chair, International Association of Privacy Professionals KnowledgeNet Chapter, Minneapolis-St. Paul
- Past President, numerous Bar Association Committees and Divisions

Community Involvement

- Minnesota State Cycling Champion – Road Race (2009)
- Minnesota State Cycling Champion – Criterium (2009)

Accolades

- Listed in *Best Lawyers in America*©, 2008-2016
- Listed as a Minnesota Super Lawyer, 2011-2015

Education & Admissions

United States Naval Academy (B.S., Engineering, 1972), with Distinction

University of Wisconsin Law School (J.D., 1975), with Honors

Admissions

- Minnesota
- Wisconsin

- Minnesota Supreme Court
- Wisconsin Supreme Court
- Minnesota Federal District Court
- Wisconsin Federal District Court
- U.S. Court of Appeals for the Eighth Circuit
- U.S. Court of Claims
- U.S. Supreme Court

Industries & Practices

- Closely Held Businesses
- Energy
- Environmental

- Food & Agribusiness
- Government Enforcement & Corporate Investigations
- Health Care
- Insurance Law
- Mining & Natural Resources
- Cybersecurity, Privacy & Social Media
- Public-Private Project Development
- Telecommunications
- Telecommunications

News & Resources

Insights

Dorsey Partner Bob Cattanach Comments on New EU Privacy Rule

December 14, 2015

Dorsey Partner Bob Cattanach Discusses Cybersecurity Issues After Paris Attacks

November 20, 2015

Joe Hall, Bob Cattanach and Brad Hammer author article on energy and privacy law: "So, who owns your energy-use data?"

WindPower Engineering and Development

October 2015

Dorsey Partner Bob Cattanach Comments on US-China Agreement on Cybertheft

October 6, 2015

Dorsey Partner Bob Cattanach Discusses DC Court Lifting NSA Ruling

August 28, 2015

Dorsey Partner Bob Cattanach Comments on FTC's Data Security Win

August 24, 2015

45 Dorsey Lawyers in Minneapolis and Fargo Selected for Inclusion in *The Best Lawyers in America*® 2016 and *Best Lawyers of the Year*

August 17, 2015

Five Steps to Prepare for a Data Breach

August 10, 2015

Dorsey Partner Bob Cattanach Discusses Napa County Wineries Data Breach

July 12, 2015

Super Lawyers Recognizes 39 Dorsey Lawyers in Minneapolis

July 7, 2015

Dorsey Partner Bob Cattanach Discusses the Patriot Act

June 1, 2015

Dorsey Partner Bob Cattanach Remarks on Court's NSA Ruling

May 7, 2015

Dorsey Partner Bob Cattanach Comments on Cyber Sharing Bills

April 23, 2015

Dorsey Partner Bob Cattanach Comments on AT&T $25 Million Data Breach

April 9, 2015

AT&T Settles with FCC for $25 Million in Landmark Privacy and Data Breach Agreement

April 8, 2015

Dorsey Partner Bob Cattanach Discusses Who is at Risk for Cyberattacks

January 30, 2015

Dorsey Partner Bob Cattanach Comments on Lack of Broadband Access in Rural America

January 29, 2015

Dorsey Partner Bob Cattanach Comments on Call for Bipartisan Effort to Cybersecurity Issues

January 21, 2015

Dorsey Partner Bob Cattanach Remarks on Obama's Cybersecurity, Privacy Plans

January 16, 2015

Proposed Federal Breach Notification Law: *Panacea or Flash in the Pan?*

January 16, 2015

Events & Speaking Engagements

Dorsey Partner Bob Cattanach to Present at Dorsey's Energy Industry Group Webinar Series on "How to Prepare for Cybersecurity Threats in the Energy Sector"

Tuesday, January 19, 2016

Dorsey Seminar on Cyber Intrusions and Data Security

June 26, 2014

Privacy & Technology Commerce Breakfast Briefing

March 12, 2014

Select Client Presentations

- "Dorsey & Whitney LLP DorsEdiscovery Forum," Dorsey & Whitney LLP Seminar, January 28, 2015
- "Dorsey & Whitney LLP Cybersecurity Seminar," Dorsey & Whitney LLP Seminar, November 12, 2014
- "Company Computers Under Attack: Big Dollars and Private Data Are Being Stolen Every Day: What Are You Doing About It?", Dorsey & Whitney LLP Webinar, June 26, 2014
- "Privacy & Technology Commerce," Dorsey & Whitney LLP Breakfast Briefing, March 12, 2014
- "Once More Into the Breach: Managing Risks When Your Company's Data Has Been Compromised," Dorsey & Whitney Corporate Counsel Symposium, 2013
- Numerous CLE presentations on Regulatory Litigation and Enforcement

MICHAEL GOMEZ

Principal

KPMG LLP
1801 K Street NW
Suite 12000
Washington, DC 20006

Tel 202-533-5007
Fax 202-330-5425
Cell 202-999-9383
michaelgomez@kpmg.com

Function and Specialization

Skilled technology professional with significant experience in information technology and operational technology security, governance, risk management and compliance.

Representative Clients

- AEP
- BP
- Chevron
- ConEdison
- DTE
- Exelon
- FirstEnergy
- NextEra Energy Inc.
- Pacific Gas & Electric
- SCANA
- Sempra Energy
- Southern Company

Education, Licenses & Certifications

- BS, Master of Business Administration
- Project Management Professional (PMP)

Background

Michael Gomez is KPMG's Information Protection and Business Resilience (IPBR) lead Partner for the Energy sector. Mr. Gomez is recognized within the energy industry for performing or managing numerous cyber maturity assessments, vulnerability assessments and guiding the implementation of large and complex compliance programs. Mr. Gomez is often quoted in print media on the threat of cyber security to the Energy industry.

Professional and Industry Experience

Mr. Gomez is a dedicated energy industry practitioner who has focused on improving operational performance by delivering business, operational technology (OT) and information technology (IT) solutions.

Representative engagements include:

- Engagement Advisory Partner for a large Midwest utility – currently supporting the PMO in the execution of NERC CIPv5. Specific responsibilities include maintain knowledge and provide insight into NERC CIP implementation leading practices. Act as a resource to the Engagement Leadership team and provide expanded delivery on all matters to deal with NERC CIP.
- Lead Engagement Partner for a West coast utility - created a governance structure to evaluate risk of the ICS environment. Established a customized set of controls by leveraging NIST 800-53 and ISO-99 for the client's gas, solar and wind assets. Evaluated ICS assets against the controls to identify gaps, created remediation plan. Currently assisting client with the execution of remediation plan.
- Engagement Partner for a Midwest utility – currently assessing 12 critical assets, including 11 plants and the control center, to determine the control and process gaps between NERC CIP requirements and the current processes at the plant. Gap assessment will give an indication of process maturity and will assist in building a foundation of a NERC CIP program and roadmap.
- Engagement Partner for a West coast utility – designed, built and implemented an Archer GRC solution to support NERC CIPv3 and CIPv5 requirements. Engagement required active collaboration and coordination across the company's lines of business and IT.
- Engagement Manager for an Oil Super Major – assessed the global cyber security controls of the process control network for the upstream. Developed detail remediation plan which was presented to the executive committee.
- Engagement Partner for a southern utility – lead the creation of a companywide unified controls framework inclusive of NERC CIP, NIST and NEI 08-09. Managed the evaluation of a smart grid cyber vulnerability assessment. Created mitigation packages and made remediation recommendations for IT and Operations.
- Engagement Partner for a Midwest utility – reviewed the design of the NERC CIP compliance program, infrastructure and initiatives. Assessed the structure of key NERC compliance program elements incorporating a gap analysis, evaluating such elements against relevant regulatory frameworks as well as industry leading practices.
- Engagement Partner for a midstream pipeline company – reviewed ICS governance and existing control framework to determine key control area gaps. Conducted vulnerability assessment to assess the current security architecture and develop a heat map of risk and prioritize. Reviewed and assessed the 2-3 ICS roadmap strategy and provided actionable recommendations.

RONALD E. PLESCO, JR., ESQ.

Principal and National Lead, Cyber Investigations
KPMG LLP
30 N. Third Street, Suite 1000
Harrisburg, PA 17101

Tel 717-260-4602
Fax 717-828-1225
Cell 412-953-0777
rplesco@kpmg.com

Assistant: Karla Wissler – kwissler@kpmg.com

Function and Specialization

Risk Consulting
Cyber Threat Intelligence
Cyber Investigation
Online Fraud and Money Laundering

Education, Licenses & Certifications

- Juris Doctorate - Oklahoma City University School of Law, Oklahoma City, Oklahoma (Academic Juris Prudence Award in trial practice, Academic Achievement Award, ATT Campus of Tomorrow fellow)
- Bachelors of Arts, History and Political Science - Washington and Jefferson College, Washington, Pennsylvania

Professional Affiliations

- Commissioned Member, Pennsylvania Homeland Security Council
- Past President, Central Pennsylvania Infragard Chapter
- Past Chief Counsel/Technology Counsel, International Association of Financial Fraud Investigators
- NCFTA Board Member & Chair
- Economic Crime Institute, Utica College Board Member
- Infragard Board Member
- Member, American Bar Association
- Member, American Bar Association Science and Technology Committee (member sub-committees or cyber crime and privacy)
- Member, American Society for Industrial Security High Technology Crimes Investigators
- Member, International Association of Privacy Professionals

Background

Ron is an internationally known information security and privacy attorney with 17 years' experience in cyber investigations, information assurance, privacy, identity management, computer crime and emerging cyber threats and technology solutions. Ron is a Principal and the National Lead of the KPMG Cyber Investigations practice. Ron joined KPMG in 2012 after a distinguished career in the private and public sectors and is a frequent speaker nationally. Prior to joining KPMG, Ron was the CEO of the National Cyber Forensics and Training Alliance (NCFTA), where he managed the development of intelligence that led to over 400 worldwide cyber crime arrests in four years and prevented over $2 billion in fraud. Notable NCFTA intelligence-led arrests include Ghost Click, Anonymous, Coreflood and multiple online frauds.

Professional and Industry Experience

Ron is a seasoned professional and recognized leader with experience in:

- Cyber Incident response and investigation
- Cyber Threat Intelligence
- Cyber Crime Threats
- Credit Card Fraud
- Identity and Information Theft
- Identity Management
- Information Assurance
- Risk and Compliance
- Brand Development/Management
- Privacy

Publications and Articles

- *"Mitigating the Risk of Wire Fraud,"* Treasury and Risk Magazine, 2015
- *"Alleviating Cyber Attacks through Comprehensive Analysis,"* CIO Review Magazine 2015
- *"Cyber Security Experts Try to Predict Hackers' Next Moves,"* Pittsburgh Tribune, 2015
- *"Cyber Security for Today's Healthcare Organizations,"* Risk and Compliance Magazine, 2015
- *"Cyber Security for Small Business,"* Knowledge@Wharton SiriusXM Radio, 2015
- *"Responding to Technology Risks – Cyber Security,"* Technology Risk Radar, 2014
- Privacy Piracy Radio Cyber Investigations Interview, 2015
- *"KPMG LLP US Named 2014 Cyber Investigations Team of the Year,"* Acquisition International Finance Awards, 2014
- *"The Best of the Rest of Black Hat: The Enterprise View,"* InformationWeek Dark Reading Radio, 2014
- *"Necessity of Proactive Cybersecurity Measures to Meet Growing Threats",* San Diego Business Journal, 2014
- *"Cyber Attacks Know no Barriers",* Metropolitan Corporate Counsel, National Edition, 2013
- *"Criminal Public-Private Partnerships, Why Can't We Do That?",* Georgetown Journal of International Affairs, 2011
- *"International Guide to Combating Cyber Crime",* American Bar Association Publications, 2010

- Member, International Association of Chiefs of Police Member, International Association of Financial Fraud Investigators
- Member, Pennsylvania Bar Association
- Member, RSA Chairman's Circle

Notable Media Appearances

- CBS Evening News
- CNBC
- 60 Minutes
- ARD Germany
- Canadian Broadcasting Company

Honors and Awards

- Winner, Most Influential People in Security, *Security* Magazine, December 2010
- Winner, Editors' Choice Award, *Secure Computing* Magazine, 2010

How to Prepare for Cybersecurity Threats

January 19, 2016

Robert Cattanach, Partner, Dorsey & Whitney LLP

Michael Gomez, Partner, KPMG

Ron Plesco, National Lead, Cyber Investigations, Intelligence & Analytics, KPMG

Meet the Panel

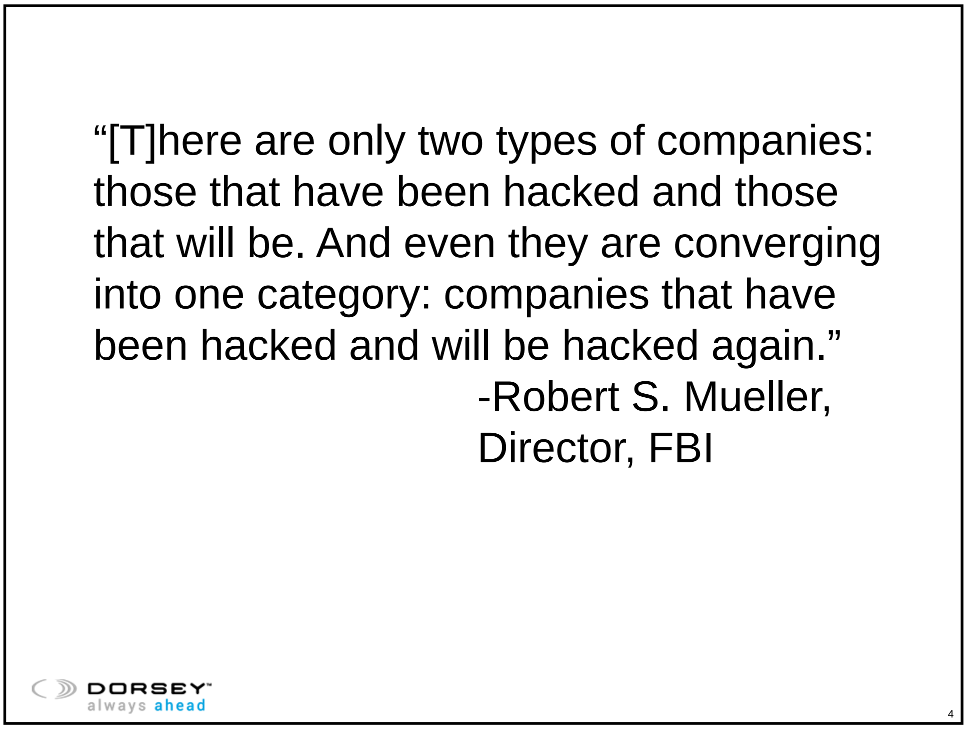
Bob Cattanach
Partner
Dorsey & Whitney LLP
Minneapolis, Minnesota
(612) 340-2873
cattanach.robert@dorsey.com

Michael Gomez
Principal
KPMG LLP
Washington, DC
(202) 533-5007
michaelgomez@kpmg.com

Ronald Plesco
Principal & National Lead,
Cyber Investigations
KPMG, LLP
Harrisburg, Pennsylvania
(717) 260-4602
rplesco@kpmg.com

KPMG slides not authorized for release.

3

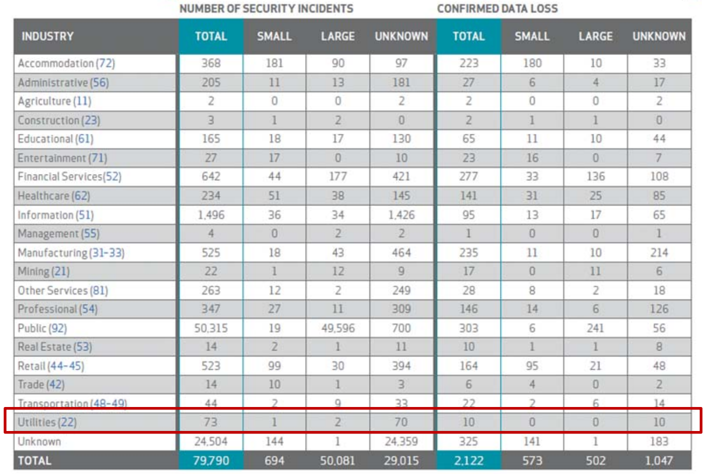


“[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

-Robert S. Mueller,
Director, FBI

4

Security Incidents* By Industry



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services(52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

* Security incident: Any compromise of the confidentially, integrity, or availability of an information system.
Data breach: A confirmed disclosure of information (not just exposure) to an unauthorized party. *Source: Verizon Data Breach Investigation Report 2015.*

Data Breach Trends

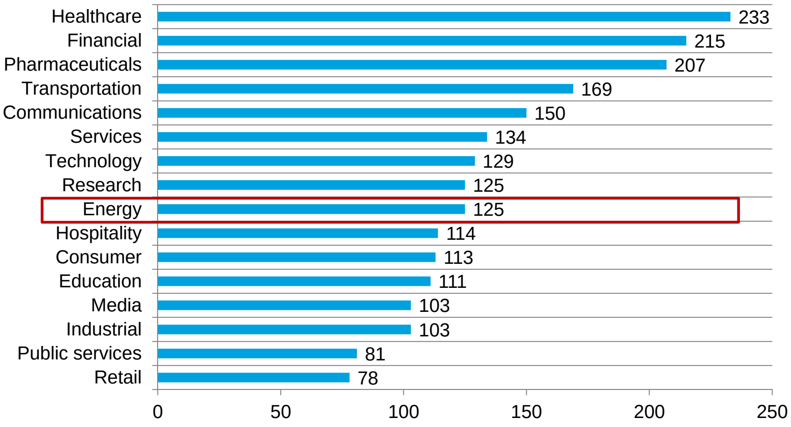
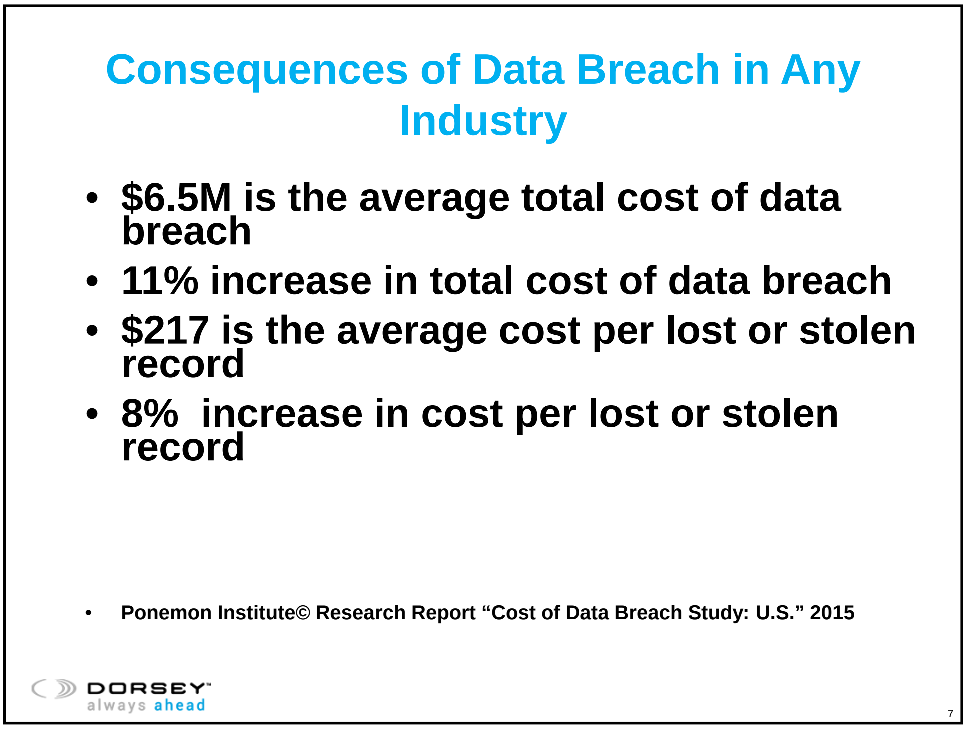


Figure 4. Per capita cost by industry classification
Consolidated view (n=277). Measured in US$
Source: Ponemon Institute/Symantec, 2013 Cost of a Data Breach Study

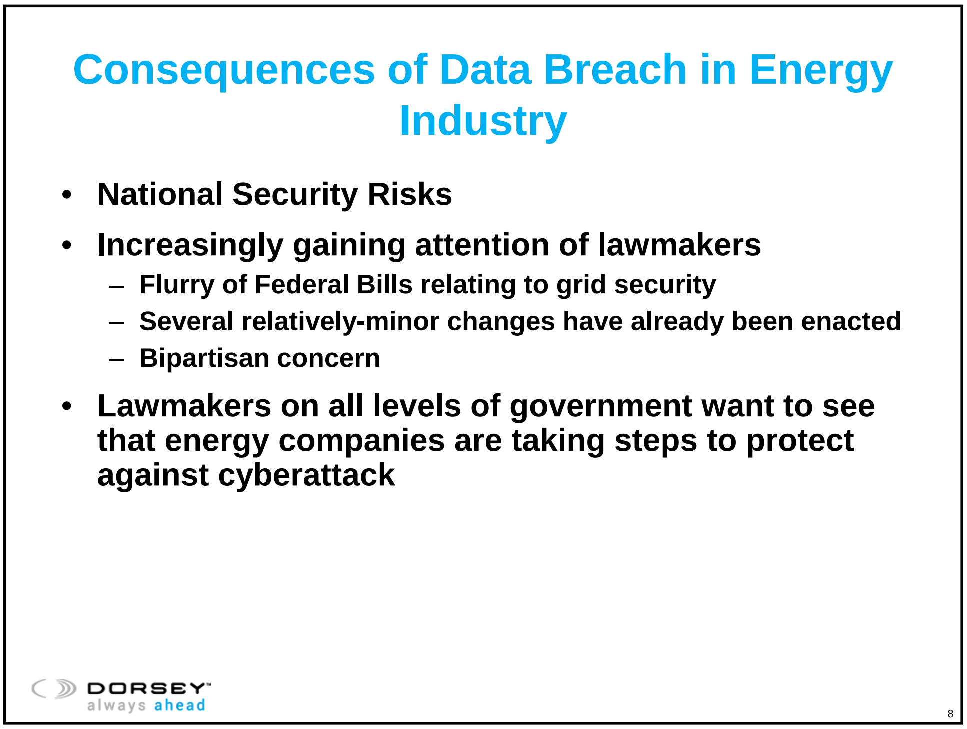


Consequences of Data Breach in Any Industry

- $6.5M is the average total cost of data breach
- 11% increase in total cost of data breach
- $217 is the average cost per lost or stolen record
- 8% increase in cost per lost or stolen record

- Ponemon Institute© Research Report “Cost of Data Breach Study: U.S.” 2015

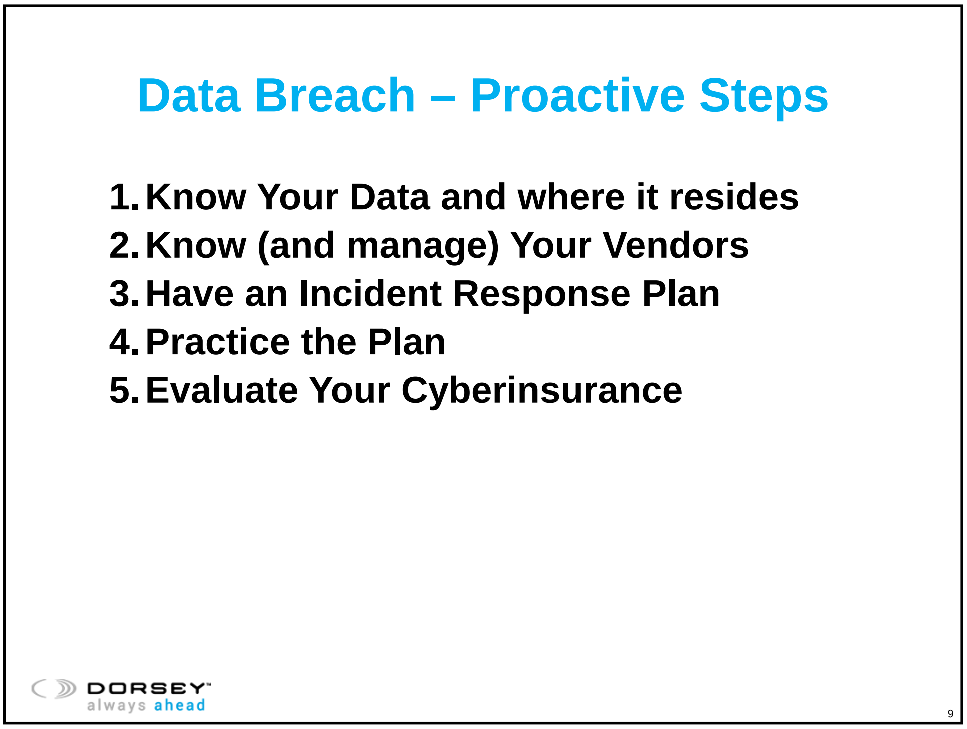
DORSEY™ always ahead



Consequences of Data Breach in Energy Industry

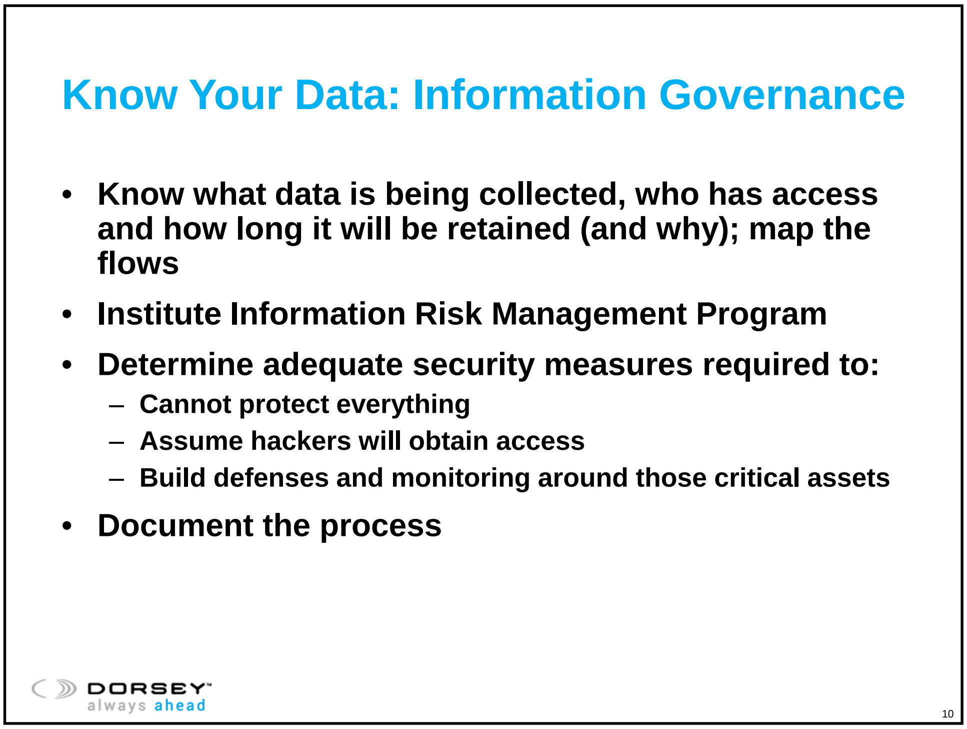
- National Security Risks
- Increasingly gaining attention of lawmakers
  - Flurry of Federal Bills relating to grid security
  - Several relatively-minor changes have already been enacted
  - Bipartisan concern
- Lawmakers on all levels of government want to see that energy companies are taking steps to protect against cyberattack

DORSEY™ always ahead



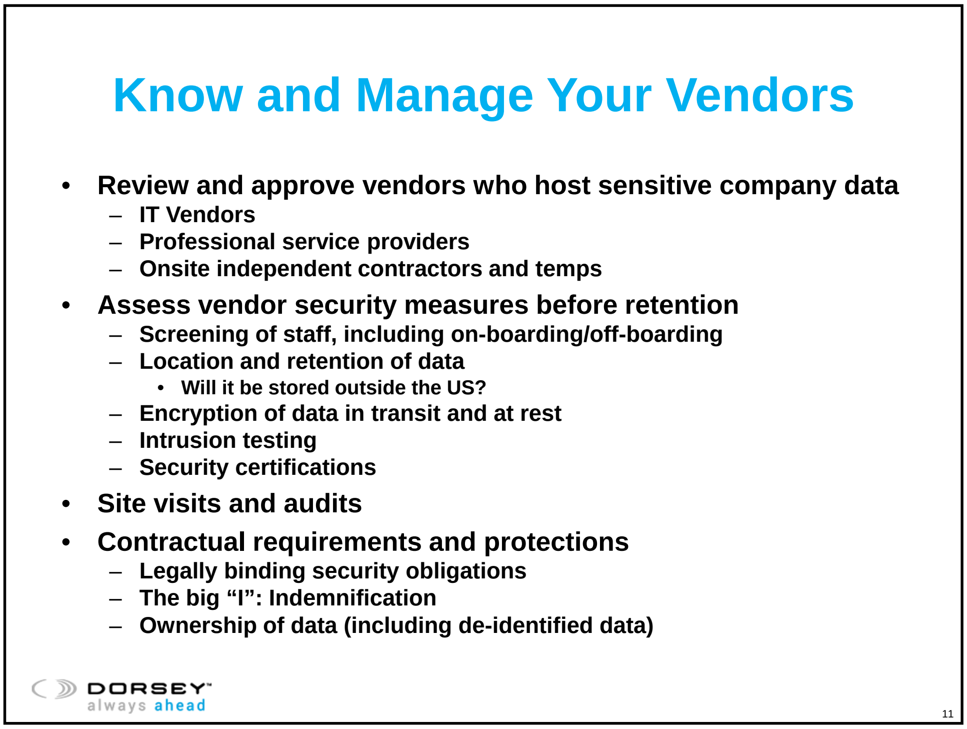
Data Breach – Proactive Steps

1. Know Your Data and where it resides
2. Know (and manage) Your Vendors
3. Have an Incident Response Plan
4. Practice the Plan
5. Evaluate Your Cyberinsurance



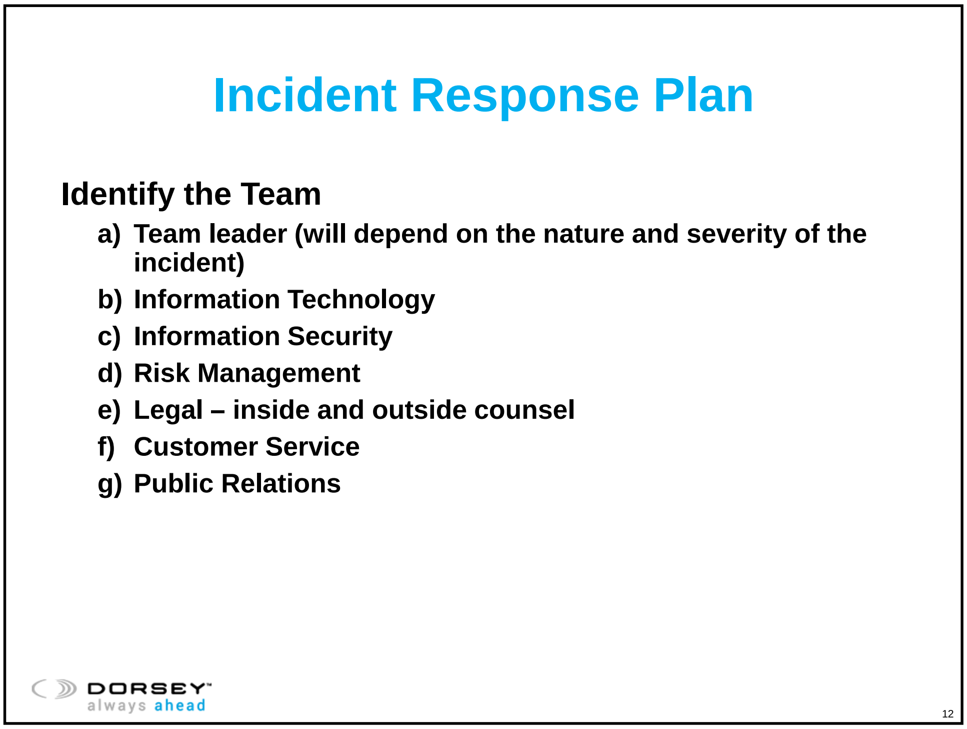
Know Your Data: Information Governance

- Know what data is being collected, who has access and how long it will be retained (and why); map the flows
- Institute Information Risk Management Program
- Determine adequate security measures required to:
  - Cannot protect everything
  - Assume hackers will obtain access
  - Build defenses and monitoring around those critical assets
- Document the process



Know and Manage Your Vendors

- Review and approve vendors who host sensitive company data
  - IT Vendors
  - Professional service providers
  - Onsite independent contractors and temps
- Assess vendor security measures before retention
  - Screening of staff, including on-boarding/off-boarding
  - Location and retention of data
    - Will it be stored outside the US?
  - Encryption of data in transit and at rest
  - Intrusion testing
  - Security certifications
- Site visits and audits
- Contractual requirements and protections
  - Legally binding security obligations
  - The big “I”: Indemnification
  - Ownership of data (including de-identified data)



Incident Response Plan

Identify the Team

a) Team leader (will depend on the nature and severity of the incident)

b) Information Technology

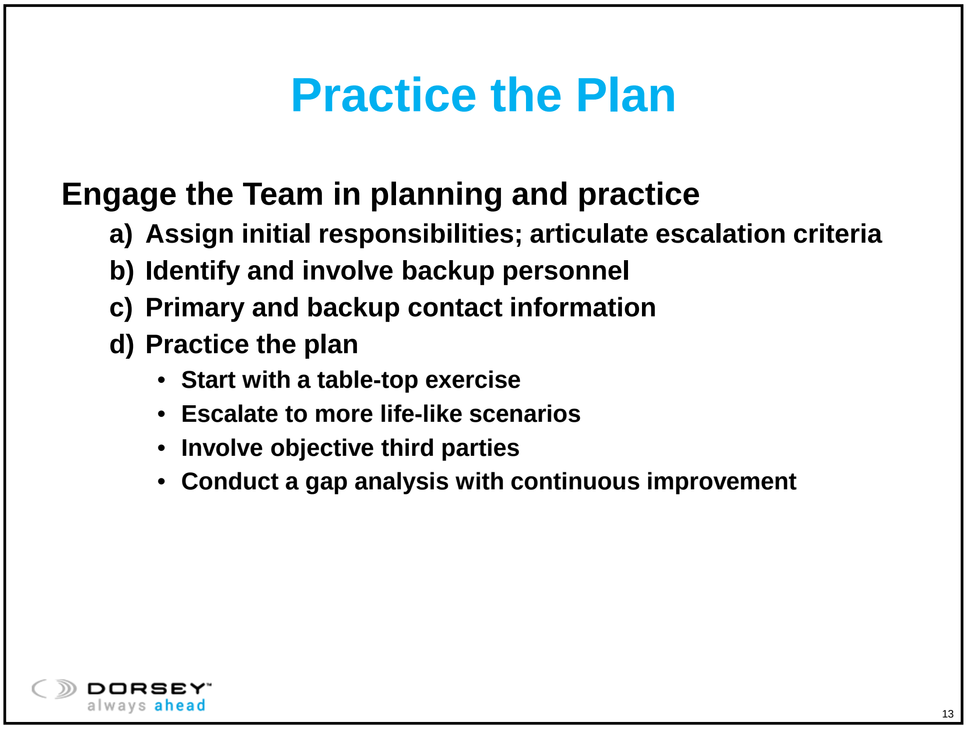
c) Information Security

d) Risk Management

e) Legal – inside and outside counsel

f) Customer Service

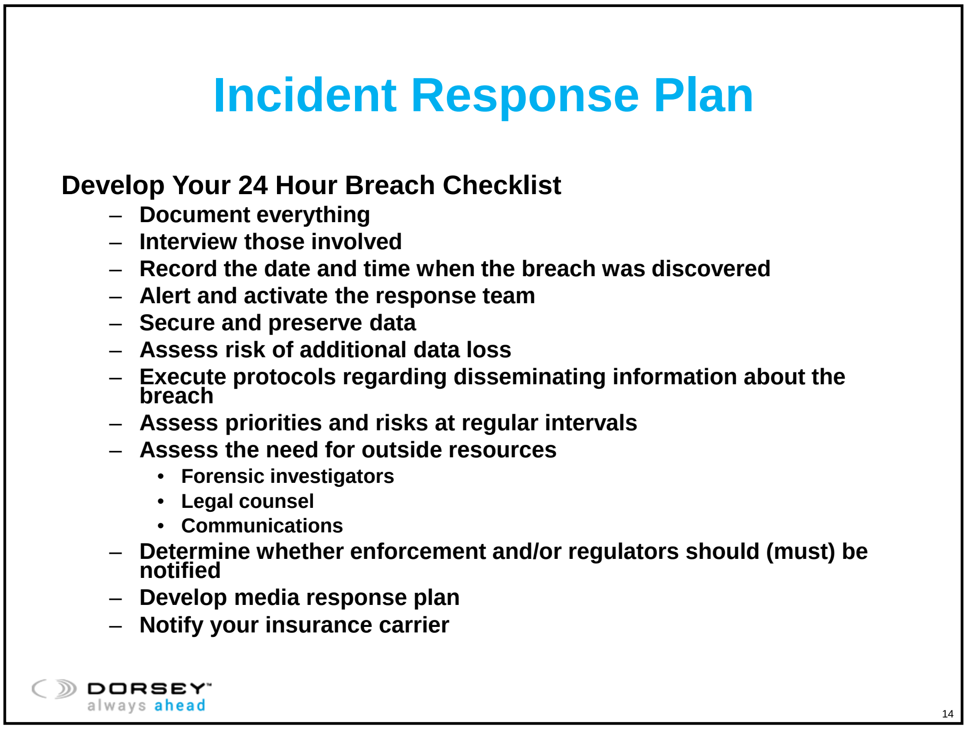
g) Public Relations



Practice the Plan

Engage the Team in planning and practice

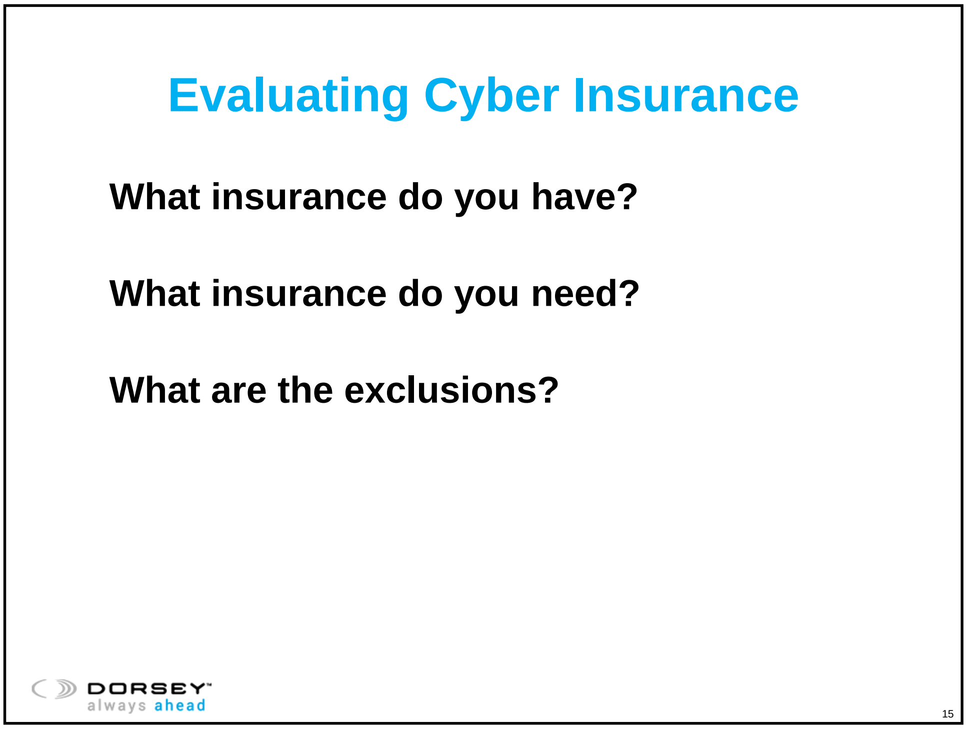
a) Assign initial responsibilities; articulate escalation criteria
b) Identify and involve backup personnel
c) Primary and backup contact information
d) Practice the plan
  - Start with a table-top exercise
  - Escalate to more life-like scenarios
  - Involve objective third parties
  - Conduct a gap analysis with continuous improvement



Incident Response Plan

Develop Your 24 Hour Breach Checklist

- Document everything
- Interview those involved
- Record the date and time when the breach was discovered
- Alert and activate the response team
- Secure and preserve data
- Assess risk of additional data loss
- Execute protocols regarding disseminating information about the breach
- Assess priorities and risks at regular intervals
- Assess the need for outside resources
  - Forensic investigators
  - Legal counsel
  - Communications
- Determine whether enforcement and/or regulators should (must) be notified
- Develop media response plan
- Notify your insurance carrier

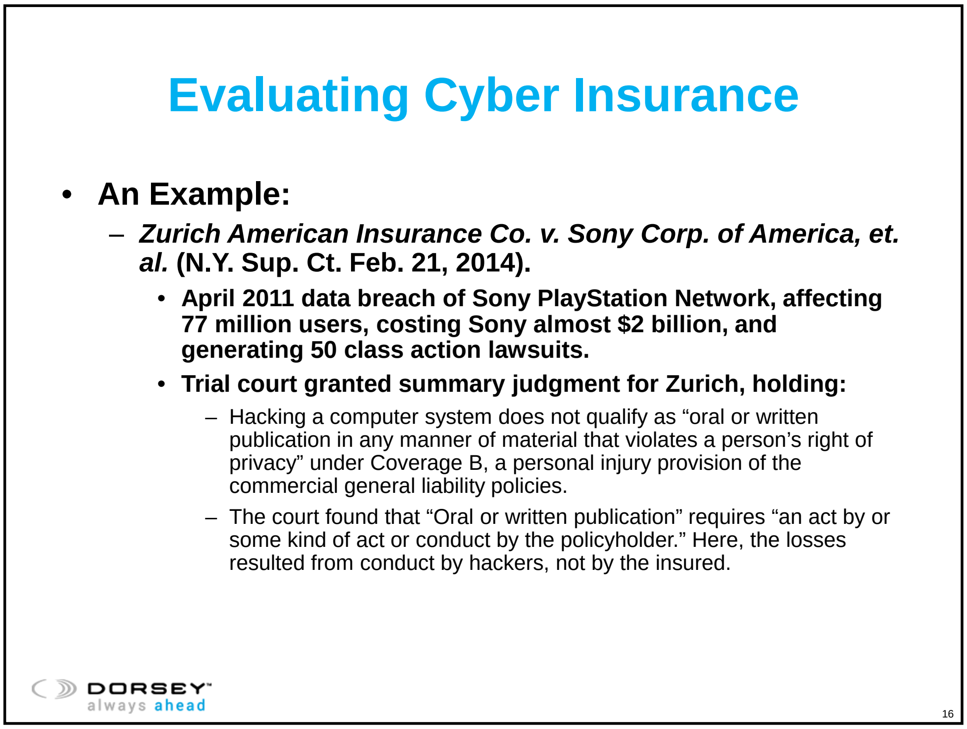


Evaluating Cyber Insurance

What insurance do you have?

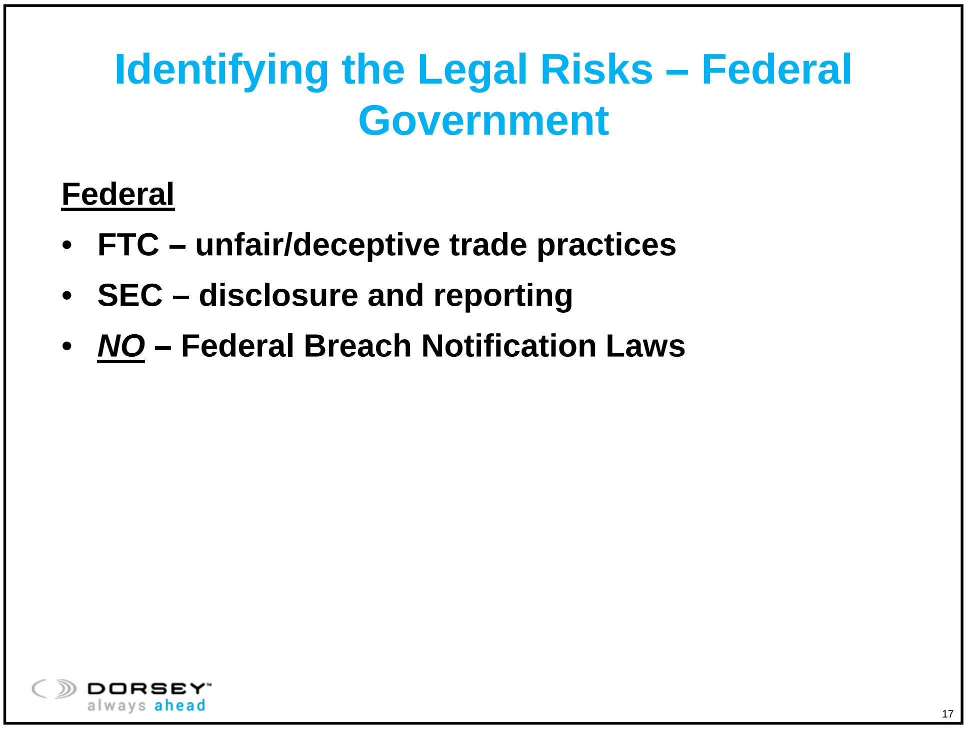
What insurance do you need?

What are the exclusions?



Evaluating Cyber Insurance

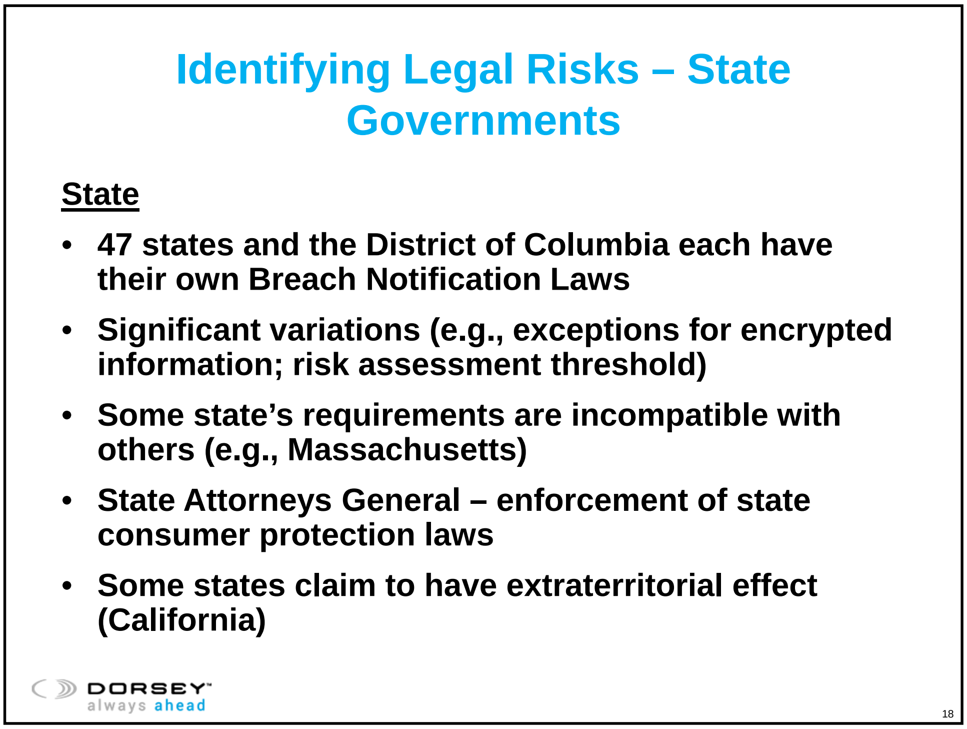
- **An Example:**
  - ***Zurich American Insurance Co. v. Sony Corp. of America, et. al.* (N.Y. Sup. Ct. Feb. 21, 2014).**
    - **April 2011 data breach of Sony PlayStation Network, affecting 77 million users, costing Sony almost $2 billion, and generating 50 class action lawsuits.**
    - **Trial court granted summary judgment for Zurich, holding:**
      - Hacking a computer system does not qualify as “oral or written publication in any manner of material that violates a person’s right of privacy” under Coverage B, a personal injury provision of the commercial general liability policies.
      - The court found that “Oral or written publication” requires “an act by or some kind of act or conduct by the policyholder.” Here, the losses resulted from conduct by hackers, not by the insured.



Identifying the Legal Risks – Federal Government

Federal

- **FTC – unfair/deceptive trade practices**
- **SEC – disclosure and reporting**
- ***NO* – Federal Breach Notification Laws**



Identifying Legal Risks – State Governments

State

- **47 states and the District of Columbia each have their own Breach Notification Laws**
- **Significant variations (e.g., exceptions for encrypted information; risk assessment threshold)**
- **Some state’s requirements are incompatible with others (e.g., Massachusetts)**
- **State Attorneys General – enforcement of state consumer protection laws**
- **Some states claim to have extraterritorial effect (California)**

KPMG

cutting through complexity

Connecting the dots:

A proactive approach to cybersecurity oversight in the boardroom

kpmg.com

Ron is a nationally known information security and privacy attorney with 16 years of experience in information assurance/privacy, identity management, computer crime, and emerging cyber threats and technology solutions. Ron previously served as the CEO of the National Cyber Forensic & Training Alliance (NCFTA) and currently leads KPMG's cyber investigations practice. He is a frequent speaker internationally on cybercrime.

Ron Plesco
Principal
717-260-4602
rplesco@kpmg.com

Michael Gomez is KPMG's Information Protection and Business Resilience (IPBR) lead Partner for the Energy sector. Mr. Gomez is recognized within the energy industry for performing or managing numerous cyber maturity assessments, vulnerability assessments and guiding the implementation of large and complex compliance programs. Mr. Gomez is often quoted in print media on the threat of cyber security to the Energy industry

Michael Gomez
Principal
202-533-5007
michaelgomez@kpmg.com

Connecting the dots:

A proactive approach to cybersecurity oversight in the boardroom

Cyber attacks and data leakage are daily threats to organizations globally, reminding us that we are all potential targets of this type of threat. Attorneys are discussing the potential risk of individual liability for corporate directors who do not take appropriate responsibility for oversight of cybersecurity[1]. Investors and regulators are increasingly challenging boards to step up their oversight of cybersecurity and calling for greater transparency around major breaches and the impact they have on the business.

Given this environment, it is not surprising that cyber risk is now near the top of board and audit committee agendas. According to the KPMG 2014 Global Audit Committee Survey, nearly 45 percent of audit committees in the United States have primary oversight responsibility for cybersecurity risk; yet, only 25 percent say that the quality of the information they receive about cybersecurity is good. So a critical question for every audit committee is: What information do they require—or is most critical—in assessing whether management is appropriately addressing cyber risk? Certainly, directors need to hear from a Chief Information Security Officer (CISO) or CIO who is knowledgeable and can help them see the big picture. But what should be the key areas of focus?

In our experience board members are wondering: Am I asking the right questions? How do I get comfortable? Are we doing enough? How do I know we are doing the right things? Are we making the right decisions?

Cybersecurity: a business and boardroom priority

By now, corporate boards have woken up to the call that they must address cybersecurity issues on their front lines, as it is not just an Information Technology (IT) issue. In fact, cyber risks are an enterprise-wide risk management issue.

SEC Commissioner Luis Aguilar's 2014 speech,[2] during which he urged boards to sharpen their focus on cyber risks, rings even more true today and serves as a warning for the future:

> *"…boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."*

Aguilar addressed what boards can and should be doing to oversee cyber risk, pointing to a potential knowledge gap:

> *"Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. Yet, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues."*

[1] "The Morning Risk Report: Cybersecurity Responsibility Falling to Boards," Risk & Compliance Journal, The Wall Street Journal, March 4, 2015, http://blogs.wsj.com/riskandcompliance/2015/03/04/the-morning-risk-report-cybersecurity-responsibility-falling-to-boards/.

[2] U.S. Securities and Exchange Commission, speech transcript, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," by SEC Commissioner Luis A. Aguilar, "Cyber Risks and the Boardroom" Conference, New York Stock Exchange, New York, NY, June 10, 2014, http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

We believe the process for closing that gap should not be a mystery. Taking a proactive approach to improving cybersecurity governance—connecting the dots between IT and the business, and providing the board with the information it needs—can help position the company and the board to more selectively address the evolving threat and implications of a major cybersecurity breach.

What is at stake?

Since many global organizations have been victims of cyber crime over recent years, board oversight of cybersecurity is no longer just a leading practice—it is a necessity. Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in this area. Regulators expect personal information to be protected and systems to be resilient to both accidental data leakage and deliberate attacks.

Potential impacts and possible implications for the board include:

- **Intellectual property losses** including patented information and trademarked material, client lists, and commercially sensitive data
- **Legal expenses** including damages for data privacy breaches/compensation for delays, regulatory fines and the cost associated with defense
- **Property losses** of stock or information leading to delays or failure to deliver
- **Reputational loss** which may lead to a decline in market value, and loss of goodwill and confidence by customers and suppliers
- **Time lost** and distraction to the business due to investigating how the breach occurred and what information (if any) was lost, keeping shareholders advised and explaining what occurred to regulatory authorities
- **Administrative cost** to correct the impact such as restoring client confidence, communications to authorities, replacing property, and restoring the organization's business to its previous levels.

Action steps for implementing a cybersecurity governance plan

No two corporations are the same, therefore there is no "one-size-fits-all" cybersecurity action plan. Some firms still have to take first basic steps. Others have launched cursory efforts to combat cyber crime. And a few firms have implemented robust battle plans, but there is going to always be room for improvement.

No matter where your organization falls in the spectrum, one thing is for certain—it takes much more than just an IT tool to batten down the security hatches. Fighting cyber crime requires a company-wide effort, with plans and processes that need to be implemented. There are some key governance related elements to visit and continuously revisit for consideration as this environment evolves.

Evolving board roles and responsibilities

In a recent cybersecurity survey,[3] just 22 percent of about 1,000 senior-level IT and IT security leaders say their organization's security leader briefs the board of directors on cybersecurity strategy. Sixty-six percent of the panel forecast that three years from now the organization's security leader will regularly brief the board on a recurring basis. Also, only 14 percent of respondents say their organization's security leader has a direct reporting relationship with the CEO. In contrast, 30 percent of the panel predict that the security leader will directly report to the organization's CEO three years from now.[4]

Some main considerations for the roles of board members are:

- What roles do senior leaders and the board play in managing and overseeing cybersecurity and cyber incident response, and who has primary responsibility?
- Do we have a CISO, and who does the CISO report to? Is there a direct line to the CEO?
- Do we need a separate, enterprise-wide cyber risk committee for more regular communication?

Communication frequency

A recent survey of more than 1,000 directors at public companies conducted by the National Association of Corporate Directors (NACD)[5] showed more than half (52.1 percent) of directors say they are not satisfied with the quantity of the information provided by management on cybersecurity and IT risk.

Some main considerations for the frequency of communication are:

- Is the frequency of our meetings adequate, and on a recurring basis?
- Is the frequency of our direction adequate, and on a recurring basis?
- Is the frequency of communication from management adequate, and on a recurring basis? How frequently do we receive reports?
- What is our incident response plan, and how are we learning from incidents that are happening?

Communication effectiveness

The NACD survey also noted that 35.5 percent were not satisfied with the quality of information on cybersecurity and IT risk topics, which was an increase over the previous year.[6]

Some main considerations for the effectiveness of communication are:

- Do we have a holistic, board-specific framework that "closes the loop" on effective communication throughout the organization?
- Are we asking the "right" questions and sharing the "right" information for a reliable information flow?
- What is the quality of our meetings, our direction, and communication from management?
- What kind of reports are we receiving? Are we transparent and informing our stakeholders?

[3] "2015 Global Megatrends in Cybersecurity", p. 3, sponsored by Raytheon, Ponemon institute, February 2015, http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

[4] Ibid., p. 4.

[5] "Board members unhappy with information on IT, cyber security," National Association of Corporate Directors (NACD), December 3, 2014, http://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=12551.

[6] Ibid.

Closing the loop with these three key questions

From a governance standpoint, how can the board be more effective, and close the loop in its information flow? The board must always be proactive, informed, and involved without getting overwhelmed or paralyzed. Based on our board outreach and education programs, we have found these are the three most common, high-level board oversight questions asked by the executive management and the board today:

1 What are the new cybersecurity threats and risks, and how do they affect our organization?

The first question addresses *strategic* issues from the business process and corporate objectives standpoint. It is about getting an up-to-date, detailed snapshot of the current cyber threat landscape that is understood by all. It looks at getting comfortable with cybersecurity aspects of core business decisions, cutting through the technical jargon.

2 Is our organization's cybersecurity program ready to meet the challenges of today's and tomorrow's cyber threat landscape?

The second question addresses *tactical* issues, from a program, (technical) capability, and process perspective, and how they are cascaded throughout the organization. It looks at whether the organization is doing enough due diligence to mitigate risks, depending on its risk profile.

3 What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?

The third question addresses the many *operational* issues, clarifying, prioritizing, and ultimately translating them to what it really means from a risk posture point of view and ultimately, closing the loop. This is "where the rubber meets the road," and indicates how you will know whether you are doing the right thing—so you can sleep at night more easily.

These three questions are interrelated and allow for continuous synchronization and integration as the board wants to remain agile and responsive to the evolving and changing cyber threat landscape.

KPMG's Global Cyber Maturity Framework

Cybersecurity is more than a technology problem—it is a holistic one. In response, KPMG designed a global Cyber Maturity Framework specifically to assist organizations in addressing these critical questions by combining the most relevant aspects of existing international cybersecurity standards and governance frameworks.

While we recognize the "alphabet soup" of existing framework options available (which are primarily IT or controls driven) are valuable, we believe KPMG's Cyber Maturity Framework is a broader, more thorough, and more holistic way to address board engagement and how boards can exercise their oversight responsibilities.

For example, while the National Institute of Standards and Technology (NIST) Cybersecurity Framework is beneficial for defining and assessing the control maturity of the operational aspects of a cyber program within the current environment, KPMG's Cyber Maturity Framework is specifically designed to provide strategic alignment for coordinating board and non-IT oversight and governance. Together, both frameworks provide mutual compatibility.

We regularly provide multidisciplinary assessments for boards that are focused on their business globally against these six domains: 1. Leadership and Governance, 2. Human Factors, 3. Information Risk Management, 4. Business Continuity and Crisis Management, 5. Operations and Technology, and 6. Legal and Compliance.

The application of a holistic model incorporating these six domains can bring the following benefits:[7]

- The reduction of the risk that the organization will be hit by a cyber attack from outside and the reduction of any consequences of a successful attack.
- Better decisions in the field of cybersecurity—the provision of information on measures, patterns of attack, and incidents is thus enhanced.
- Clear lines of communication on the theme of cybersecurity. Everyone knows his or her responsibilities and what must be done if incidents (or suspected incidents) occur.
- A contribution to a better reputation. An organization that is well prepared and has seriously considered the theme of cybersecurity is able to communicate on this theme in a way that inspires confidence.
- The enhancement of knowledge and competences regarding cybersecurity.
- The benchmarking of the organization in the field of cybersecurity in relation to its peers.

In addition, we offer framework mapping that is compatible with your other existing framework.

[7] *Cybersecurity, a theme for the boardroom,* p. 17, KPMG Advisory N.V. (the Netherlands), 2014, authored by KPMG partner John Hermans, http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Pages/Cybersecurity-a-theme-for-the-boardroom.aspx.

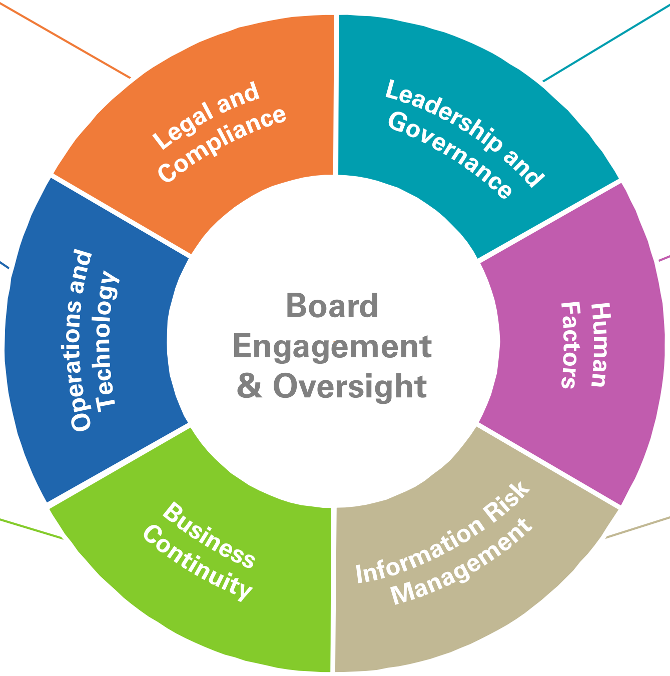
KPMG's Global Cyber Maturity Framework: Six Domains

A broad holistic framework for exercising board oversight responsibility.

Communication and direction flow through six domains
Within this Cyber Maturity Framework, a strong communications plan is focused on the details and complexity of ongoing *communication and direction* between the board and management. This helps achieve a reliable flow of information among a broad mix of stakeholders. It is not only the frequency of communication that needs to be reassessed, but also, improving the appropriate and efficient quality of communication when addressing risks.

This framework keeps in mind that security is only as strong as your weakest link—and the weakest link most often is people, whether due to someone on the inside, human error, or another human factor.

The objective is to allow for all communication—whether technical, legal, strategic, or operational—to be mutually beneficial for all stakeholders. The right questions need to be asked, and the details matter and need to be meaningful for everyone involved. Our transformative framework, with a proactive approach, helps shape the proper dialogue and overall, improves the information flow to become more transparent and sustainable—thus, closing the loop.


Legal and Compliance
Leadership and Governance
Human Factors
Information Risk Management
Business Continuity
Operations and Technology
Board Engagement & Oversight

LEGAL AND COMPLIANCE

Regulatory and international certification standards as relevant

LEADERSHIP AND GOVERNANCE

Management demonstrating due diligence, ownership, and effective management of risk

OPERATIONS AND TECHNOLOGY

The level of control measures implemented to address identified risks and reduce the impact of compromise

HUMAN FACTORS

The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture, and knowledge

BUSINESS CONTINUITY AND CRISIS MANAGEMENT

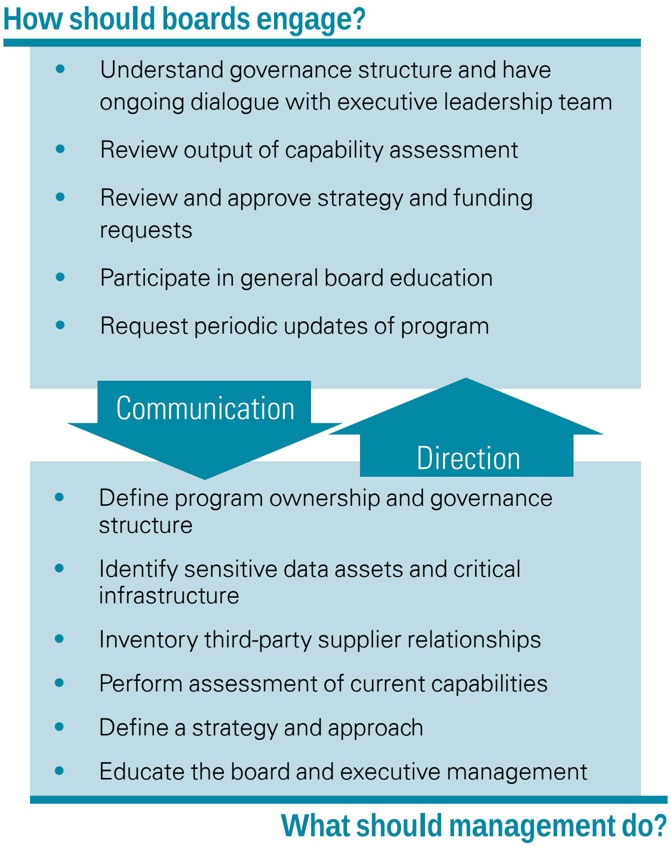
Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management

INFORMATION RISK MANAGEMENT

The approach to achieve thorough and effective risk management of information throughout the organization and its delivery and supply partners

I. LEADERSHIP AND GOVERNANCE

Management demonstrating due diligence, ownership, and effective management of risk



How should boards engage?

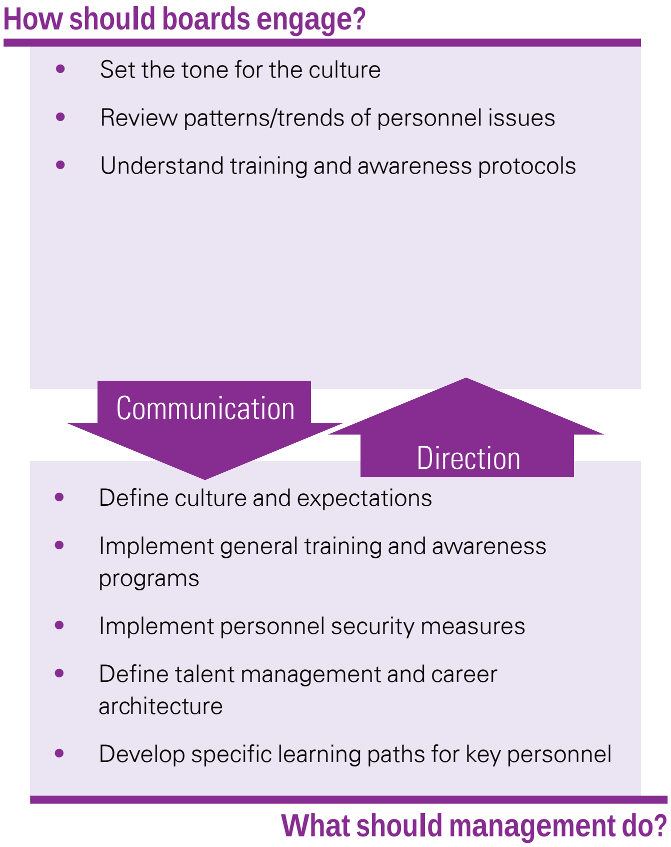
- Understand governance structure and have ongoing dialogue with executive leadership team
- Review output of capability assessment
- Review and approve strategy and funding requests
- Participate in general board education
- Request periodic updates of program

- Define program ownership and governance structure
- Identify sensitive data assets and critical infrastructure
- Inventory third-party supplier relationships
- Perform assessment of current capabilities
- Define a strategy and approach
- Educate the board and executive management

What should management do?

II. HUMAN FACTORS

The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture, and knowledge



How should boards engage?

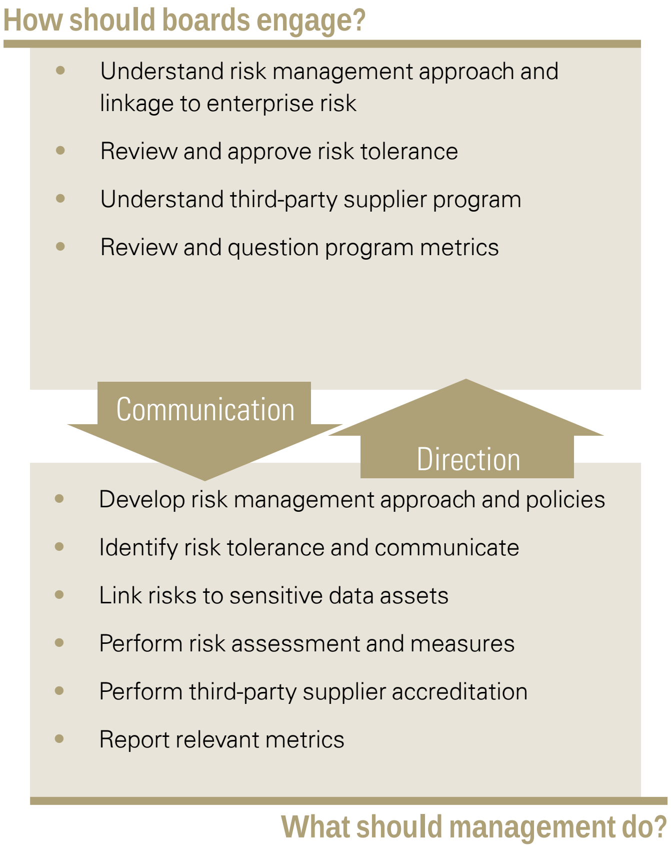
- Set the tone for the culture
- Review patterns/trends of personnel issues
- Understand training and awareness protocols

- Define culture and expectations
- Implement general training and awareness programs
- Implement personnel security measures
- Define talent management and career architecture
- Develop specific learning paths for key personnel

What should management do?

III. INFORMATION RISK MANAGEMENT

The approach to achieve thorough and effective risk management of information throughout the organization and its delivery and supply partners



How should boards engage?

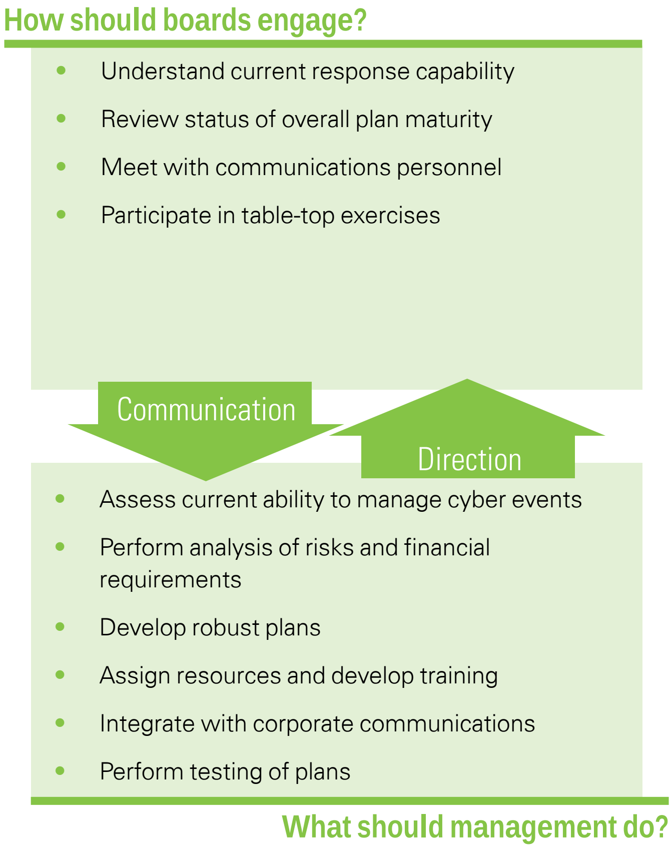
- Understand risk management approach and linkage to enterprise risk
- Review and approve risk tolerance
- Understand third-party supplier program
- Review and question program metrics

- Develop risk management approach and policies
- Identify risk tolerance and communicate
- Link risks to sensitive data assets
- Perform risk assessment and measures
- Perform third-party supplier accreditation
- Report relevant metrics

What should management do?

IV. BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management



How should boards engage?

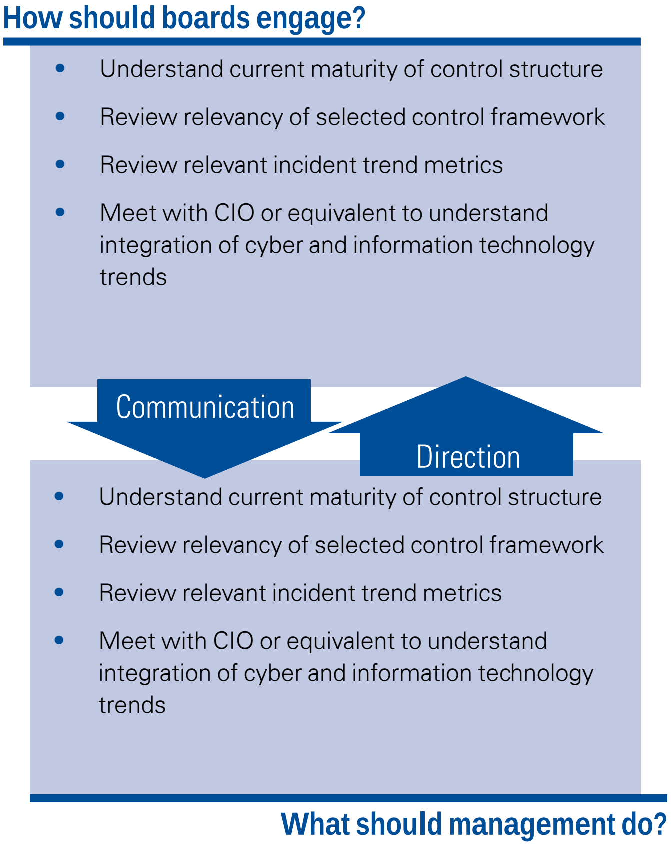
- Understand current response capability
- Review status of overall plan maturity
- Meet with communications personnel
- Participate in table-top exercises

- Assess current ability to manage cyber events
- Perform analysis of risks and financial requirements
- Develop robust plans
- Assign resources and develop training
- Integrate with corporate communications
- Perform testing of plans

What should management do?

V. OPERATIONS AND TECHNOLOGY

The level of control measures implemented to address identified risks and reduce the impact of compromise



How should boards engage?

- Understand current maturity of control structure
- Review relevancy of selected control framework
- Review relevant incident trend metrics
- Meet with CIO or equivalent to understand integration of cyber and information technology trends

Communication

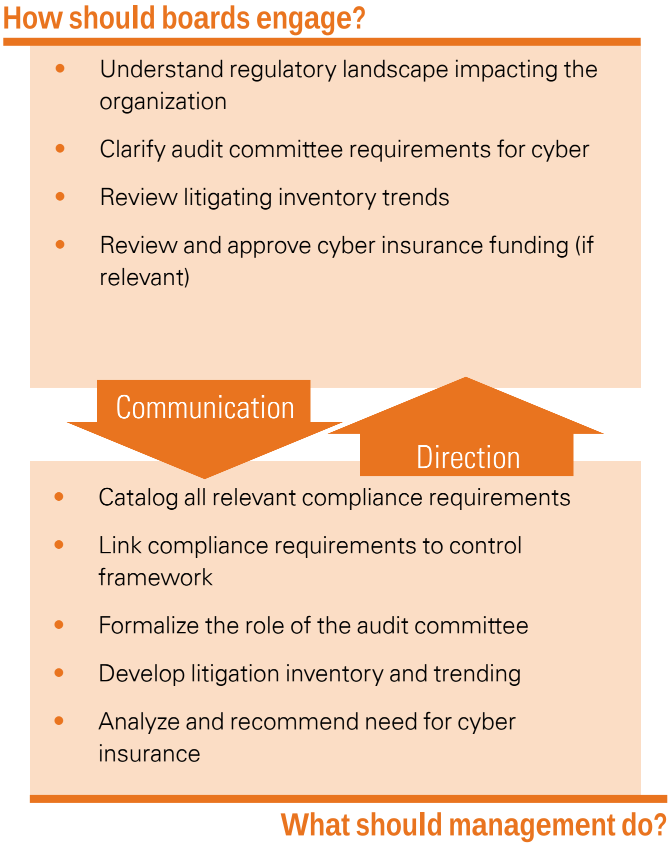
Direction

- Understand current maturity of control structure
- Review relevancy of selected control framework
- Review relevant incident trend metrics
- Meet with CIO or equivalent to understand integration of cyber and information technology trends

What should management do?

VI. LEGAL AND COMPLIANCE

Regulatory and international certification standards as relevant



How should boards engage?

- Understand regulatory landscape impacting the organization
- Clarify audit committee requirements for cyber
- Review litigating inventory trends
- Review and approve cyber insurance funding (if relevant)

Communication

Direction

- Catalog all relevant compliance requirements
- Link compliance requirements to control framework
- Formalize the role of the audit committee
- Develop litigation inventory and trending
- Analyze and recommend need for cyber insurance

What should management do?

Continue to connect the dots with metrics

It is important to assess and benchmark the value of the framework by using Key Performance Indicators (KPIs). Which KPIs are on your cyber risk dashboard? Is your organization achieving the cyber risk targets it has formulated? How do the KPIs for cyber risks relate to those of your peers?

Case study

A well-defined process for board oversight of cybersecurity

A large global manufacturer had a security breach of intellectual property in early 2014, only becoming aware of the issue when alerted by the FBI that it was monitoring transfers of large volumes of data to known hacker systems in a foreign country. After the initial triage activities took place, management had to communicate the issue to the board and explain the exposure, which was changing every day with new information that was uncovered from the investigation.

Prior to the incident, the board had only been briefed on cybersecurity on an annual basis, as part of a broader IT update from the CIO. Now the board became understandably very active in trying to understand the current state of cybersecurity risk at the company and how it can be better managed in the future.

The company hired KPMG to perform board education and a cyber maturity assessment of the organization's people, process, and technology controls to mitigate cyber threats and risks. After the initial report was complete, it was presented to the board with a full road map of prioritized remediation activities designed to close short-term gaps in the security program and execute longer-term strategies to navigate the evolving threat landscape.

After allocating funding to the initiatives on the road map, the board requested quarterly updates from management on the progress of the program in addition to an ongoing look at current operations. Management leveraged KPMG's assistance in developing dashboards of KPIs for board reporting; however, given the sensitivity around the breach and the heightened awareness of director responsibility, the board did not stop at reviewing management's materials. KPMG was hired to perform a quarterly independent "health check" of the company's progress and validate some of the information presented in key metrics. In this role, KPMG continued to be a sounding-board for the audit committee, sitting in all meetings, providing additional education on emerging trends, and validating management's assertions. Board oversight ultimately became a less complex and scary topic for directors, and the company now has a well-defined process to facilitate the communication and direction information flow between management and the board.

Conclusions

- Board oversight of cybersecurity is a required C-level activity.
- A cybersecurity governance plan needs to consider evolving board roles, as well as communication frequency and effectiveness.
- Close the loop in information flow by leveraging the three most often asked questions to address strategic, technical, and operational issues.
- KPMG's Global Cyber Maturity Framework addresses how to exercise board oversight responsibility in six enterprise-wide domains with a broader holistic approach.
- An organization's framework should efficiently and appropriately address ongoing communication and direction throughout the organization.
- Understand the enhanced value of benchmarking framework metrics and mapping the organization's framework against industry standards to stay proactive and to continue to close the loop.

9688.
7103.74
2207.6
4008.95
1038.48
6590.99
2432.55
7464.62
1041.32

Contact us

Ronald E. Plesco, Jr., Esq.
Principal and National Lead,
Cyber Investigations, Intelligence & Analytics
KPMG LLP
T: 717-260-4602
E: rplesco@kpmg.com

Michael D. Gomez
Principal
Information Protection and Business Resilience
KPMG LLP
T: 202-533-5007
E: michaelgomez@kpmg.com

kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

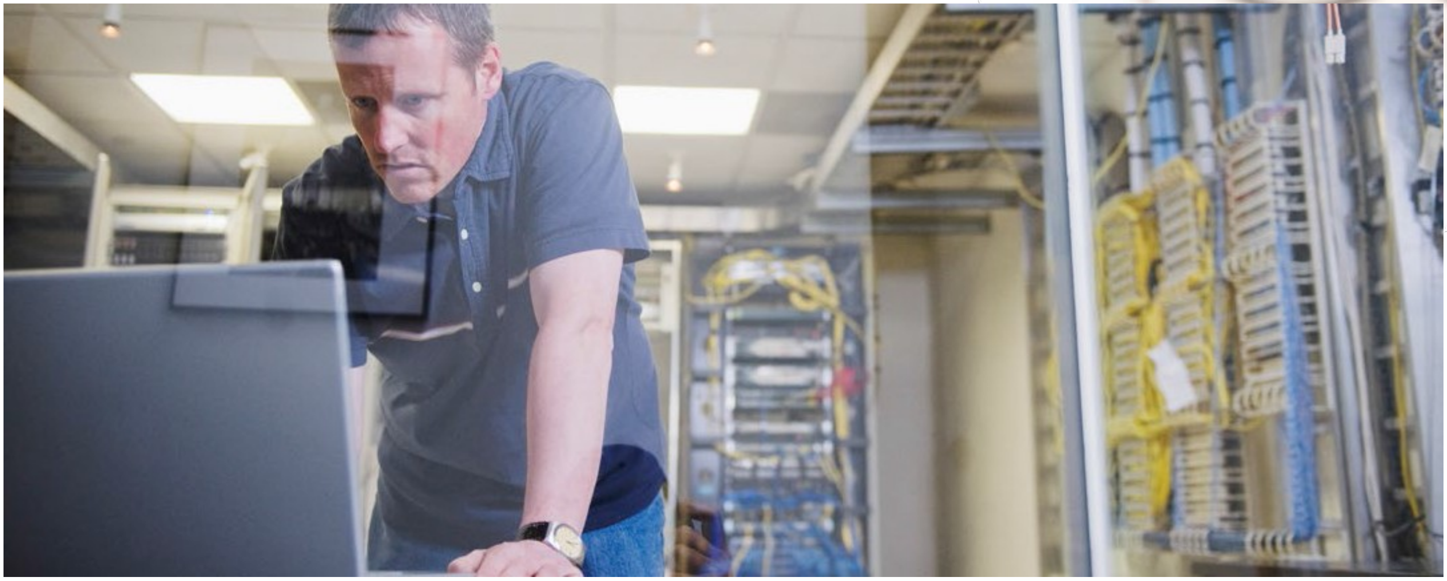
KPMG
cutting through complexity

ForensicFocus

December 2014

10 Common Cyber Incident Response Mistakes

Does your incident response program solve or exacerbate your security problems?



TODAY'S REALITY:

- A proactive and comprehensive incident response program is a critical element of information security.
- When the integrity of a computer network or information system is compromised, responding appropriately will minimize business disruptions and reduce the organization's ultimate financial burden.
- Ten major mistakes can hinder an organization's response effort to data breaches, cyber attacks and other serious security events.

In the unpredictable and fast-paced battle against cyber attackers, well-prepared incident response teams are a powerful weapon in an organization's arsenal. Responsible for assessing security systems and responding to security threats, incident response teams play a major role in resolving issues and controlling damage of system breaches, malware exposure, and other security events.

Addressing ten common incident response mistakes can help organizations determine if their incident response teams are capable of solving, rather than exacerbating, their security problems.

Mistake #1: Plans are not tailored to the organization.

Many organizations implement boilerplate incident response plans that enumerate, in extensive detail, every step that should be taken to investigate a potential incident. While this may feel thorough and reassuring, it can often overcomplicate response procedures and slow down or work against investigations. Off-the-shelf plans are often outdated and ineffective against evolving threats and changing technology.

Advice from KPMG LLP (KPMG): Organizations should establish policies, processes, and procedures that are tailored to their culture, environment, response personnel, and most importantly, business objectives. Documentation should be concise, and should evolve constantly to remain current with both external trends as well as shifts in business objectives.

Mistake #2: Plans are only used in real-world incidents.

In information security, planning only goes so far. Organizations create comprehensive incident response plans but sometimes do not test them until a real event occurs, only to find they fail at the first step. Additionally, many organizations view creating an incident response plan as a one-time event as opposed to an ongoing process. As a result, plans have incorrect information regarding tools and people, or detailed steps that do not work or are out of order.

Advice from KPMG: Organizations need to put their plans into action with regular frequency before the real event happens—similar to the way fire drills are performed.

Mistake #3: Teams are unable to communicate with the right people in the right way.

Because many IT security organizations are characterized by segmented functions such as vulnerability scanning, patching, and system administration, it can be a major challenge to find, coordinate and communicate with the key parties involved in responding to an incident.

Advice from KPMG: A centralized communication dashboard, where the incident response team can post details about the current investigation and pull the information as-needed, can help limit the disruptions of constant e-mail messaging, which can overwhelm e-mail inboxes and lead to missed messages or conflicting information. Additionally, this dashboard system can be configured to limit access or add people as needed, without sending duplicative e-mails.

Mistake #4: Teams lack skills, are wrong-sized, or mismanaged.

Both small and large organizations face challenges when it comes to choosing the right personnel to staff the incident response team. With limited security budgets, small organizations may assign incident response duties to system and network administrators, who possess technical knowledge and historical understanding of how systems operate, but no experience making business-impacting decisions amid a crisis or breach. On the other hand, large organizations struggle to allocate the most efficient number of resources to the incident response team, assuming more personnel equals greater capability. This can lead to overlapping efforts.

Advice from KPMG: Organizations should closely evaluate the need for additional training or internal recruiting assistance to help foster the proper level of experience on the incident response team. In addition, strong leaders who oversee the team should clearly define roles and responsibilities, promote greater collaboration, and improve communication to, and beyond, the team.

Mistake #5: Help desk activities can destroy critical evidence.

From strange computer behavior to frequent account lockouts to multiple antivirus alerts, computer issues that may signal a malicious code infection are often first reported to the help desk. If help desk staff members are not well versed in the needs of incident responders, their work to fix user issues may destroy key evidence. For example, installing software, running antivirus or cleaning tools, or adjusting system settings can overwrite information that may be invaluable to incident responders. Piecing together the chain of events can be impossible, especially if the initial actions were not documented.

Advice from KPMG: If they suspect a user issue may be caused by malicious code, help desk staff should capture a memory image of the system prior to making any other changes. The help desk should also be trained to document their activities in case their actions become part of an investigation.

Mistake #6: Incident response tools are inadequate, unmanaged, untested or underutilized.

Organizations may see their incident investigation and remediation processes experience unexpected delays, or even grind to a halt, if the tools teams rely on to unearth information

about affected systems and people are mismanaged or misused. Even the latest and greatest technology solution can fail to provide a consistent, reliable output without proper planning, investment, and maintenance.

Advice from KPMG: Organizations should maintain an inventory of tools in a centralized location and establish processes to help ensure timely license renewal and functional component upgrades. In addition, team members should be trained across the entire tool set on an ongoing basis. Finally, tools should be regularly assessed to determine if they can address the most current threats.

Mistake #7: Data pertinent to an incident is not readily available.

When information containing the relevant details of an attack does not exist or is not readily available, there is a cascading effect throughout the incident response process. Ultimately, the incident response team struggles to assess the impact, contain the damage, and communicate to management.

Advice from KPMG: Addressing this issue requires organizations to understand what data sources they have, what data they are capable of producing, and how they manage their data. Engaging technology owners and evaluating the asset management system are both good ways to uncover the full range of potential data sources. In addition, the incident response team should identify signaling events (e.g., failed authentication, logs purged, interactive log-on, etc.) that could provide contextual information about an incident, and establish processes for aggregating, storing, and making sense of this data.

Mistake #8: There is no "intelligence" in the threat intelligence provided to incident responders.

Threat intelligence (TI) is a buzz-worthy topic in IT security; and threat intelligence products are flying off the shelves, but many organizations find that purchasing all available threat feeds does not result in complete threat detection. Often, incident responders are overwhelmed with hashes, file names, IP addresses and other indicators, but given little or no context as to how these indicators may affect their organization.

Advice from KPMG: Organizations must integrate threat intelligence into incident response and actively work with their TI vendor help to assess if the intelligence is actionable for their organization.

Mistake #9: The incident response team lacks authority and visibility in the organization.

Political disputes can work against the incident response team's efforts, waylay the response process, and prevent timely incident resolution. It is rare that incident response teams operate with the ultimate authority to make the business changes to secure the organization. Rather, they must escalate issues to management to receive the necessary traction, sometimes as incidents worsen.

Advice from KPMG: Management must fully support the incident response team, its mission, and its activities during an investigation. Incident response should be communicated and marketed as a service that maintains the integrity of the organization, not as the group that creates more work. Additionally, other teams should nominate a primary contact to facilitate participation in the incident response process.

Mistake #10: Users are unaware of their role in the security posture of the organization.

Exploiting users is one of the most common, and easiest, ways that criminals compromise organizations. Finding a vulnerability that gives an attacker full access to a network can be a lot of work, but crafting an e-mail message that convinces a user to run malware is child's play. Unfortunately, educating users about threats only goes so far.

Advice from KPMG: Organizations should educate users not only about common exploitation practices, but also about information security's role within the organization. By doing so, users can be active participants in security. They will know where to turn and trust the process, rather than attempt to solve security problems on their own by installing untrusted tools and potentially causing greater problems across the network.

About KPMG Forensic^{SM}

KPMG comprises a global network of professionals. Many of these professionals are leaders in the Cyber Security community, helping develop the tools and methodologies used to combat cyber crime on a daily basis. Our professionals have experience working on all forms of cyber crime including insider threats, data breaches, hacktivist groups, and Advanced PersistentThreat-style intrusions by highly motivated adversaries.

KPMG is also heavily involved in the information security community.This involvement provides us with early insight into emerging issues, which we share with our clients and the project support teams as a component of our advisory role.The pragmatic advice and the services we can offer are shaped from the experience we have gained and relationships we have developed serving clients of various size, scope, and complexity.

KPMG is a preferred provider of Incident Response services to many organizations and acts as an extension of other organizations' internal teams.Since KPMG is independent (e.g., tool agnostic) and vendor neutral, clients can gain comfort in knowing that KPMG is entirely driven by our experience with similar organizations (references available) and our confidence in our ability to provide value-added assistance.

Contact us

Ronald E. Plesco
Principal and NationalLead
CyberInvestigations, Intelligence & Analytics
T: 717-260-4602
E: rplesco@kpmg.com

kpmg.com/us/forensic

KPMG Forensic is a service mark of KPMG International.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.