TABLE OF CONTENTS

EXECUTIVE SUMMARY

The relentless growth of cybercrimes against corporations reigns as one of the great corporate governance challenges of our times. Our aim in this Legal Research Report is to encourage the largest number of corporate boards and individuals in governance roles to step up and

cybersecurity governance strategies.

Consequently, we analyze the relevant concepts, principles and issues in this area, ultimately laying out a concrete set of best practices, standards and guidelines in establishing and maintaining a high quality cybersecurity governance strategy. Because law and legal principles loom large in this overall story, we accord them a central position.

Here are the questions that we answer in this report:

1. What are the legal and economic risks and impacts for businesses that accompany cybercrime and other cyber threats? What

   these risks and impacts as between public companies and private companies? What are the implications of these risks and impacts for private companies that are, or that anticipate being, funded by private equity or

   private companies, to what extent, and in what ways, should a company's legal counsel participate in the cybersecurity governance process?
   participate inƀDC /36 382055o4iegxtent, and in

   Here are the questisee quat are, on.

   cybercrime 3iime 3i78wo broad hategorequi on

- in which a

  protection of limited liability (the corporate

  or shareholders be held liable along with the corporation. This is a rarely granted remedy, but it may be imposed when the corporate protections are abused and there has been a basic injustice done to a party outside the corporation (it doesn't apply to injuries to shareholders.)

we present examples of the highest quality, gold standard approaches to cybersecurity governance. The examples are taken from the most prominent and respected systems being employed today:

-
-
-
- **FINRA Principles and E f ective Practices**
-
-

These best practices should be key reference points in designing and implementing a high-quality cybersecurity governance program. We also proceed to give some common-sense advice about setting up or improving such a program. Finally we provide advice to legal counsel on how to best represent companies with cybersecurity challenges (which means all of them).

INTRODUCTION

The rapid and constant growth of cybercrimes

- Certain industries were more vulnerable to churn;
- Detection and escalation costs are at a record high;
-
- Post data breach costs increased.[5]

Against this general background, it is no surprise that corporate leaders are now truly concerned about this problem. In a 2014 survey of nearly 500 company directors and general counsel,

second most important area for in-house counsel, after regulatory compliance. Relatedly, corporate

department.[6]

Proper cybersecurity governance requires a full and clear understanding of who is perpetrating acts of cybercrime and other injurious cyber incidents, why they engage in such acts and what methods they use. At a March 26, 2014 roundtable on cybersecurity sponsored by the SEC, one commentator, viewing the challenge globally

following answers:

-
    - our national security secrets or our intellectual property
    - Organized criminals who use sophisticated cyber tools to steal our identity and our money
    - Terrorists who want to attack our infrastructure, or
    - Hacktivists that are trying to make a social statement by stealing information and then publishing it to embarrass organizations
-
    - Destruction of data or hardware as the world saw with the Saudi Aramco or the banks in South Korea
    - Denial of service of the types that

      period of months
    -

      until ransom is paid
    - Theft where identity and money is stolen as we saw with the recent retail breaches.[7]

- The Gramm-Leach-Bliley Act (mandates privacy and security requirements for non-bank [16]
- The Children's Online Privacy Protection Act;[17]
- The CAN-SPAM Act;[18] and
- The Telemarketing and Consumer Fraud and Abuse Prevention Act.

securities laws, and the U. S. Securities and Exchange Commission (SEC) issued an extensive framework of rules and regulations to provide for implementation of those laws. The following non-exclusive list of statutes lies at the core of SEC regulation; they are also pertinent to its regulatory activities in the cybersecurity area:

- Securities Act of 1933[27] (requires that investors

  information concerning securities being

  misrepresentations, and other fraud in the sale of securities);
- Securities Exchange Act of 1934[28] (created the Securities and Exchange Commission; empowers the SEC with broad authority over all aspects of the securities industry);
- Trust Indenture Act of 1939[29] (regulates certain aspects of sales of debt securities such as

  for public sale);
- Investment Company Act of 1940[30] (regulates the organization of companies, including mutual funds, that engage primarily in investing, reinvesting, and trading in securities,

  investing public);
- Investment Advisers Act of 1940[31] (regulates investment advisers).

The SEC has been interested in cybersecurity governance for a number of years, but it has substantially increased its compliance and enforcement activities in keeping with the vastly increased need for such a regulatory enhancement. In that regard, the agency has issued several key initiatives in the area. Here are the major ones:

-

  Although the SEC Guidance

  statute or a rule or regulation, and it neither creates any new duties nor elevates the level of any existing ones, it is nonetheless very

important. This is true because it both (1) signals that the SEC considers cybersecurity to

deserve sensitivity to cybersecurity disclosure. The disclosure areas, which appear in most SEC disclosure forms, are listed in the SEC Guidance because disclosure in these areas is highly relevant to the agency's cybersecurity goals.

-

  - As a follow-up to the issuance

    in the Division of Corporation Finance began a review of the level and quality of public company disclosures of cybersecurity practices and risks. This review included

    companies of various sizes and from a wide variety of industries. Note that the receipt by a company

    that particular company's disclosure

    Well-informed companies (including those that become informed about

    high quality disclosure in the areas

-

  - Regulation S-P[33] contains the privacy rules promulgated by the SEC under Section 504 of the Gramm-Leach-Blilely Act (Act).[34]

and it has provided a suitable basis for enforcement activity in the cybersecurity area.

- Rule 30(a) of Regulation S-P is

  and investment company, and every investment adviser registered with the Commission must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records

  procedures must be reasonably

  records and information; (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to

[36]

-

  - The SEC adopted Regulation SCI[37] on November 19, 2014, in order to establish uniform requirements relating to the automated systems of

to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts. The rules include guidelines to assist entities in the formulation and maintenance of programs that would satisfy the requirements of the rules. The rules also establish special requirements for credit and debit card issuers.

- Notably, the prevention program requires the involvement of the board of directors (or committee thereof) or a designated senior manager in the approval, oversight, development, implementation and administration of the program.

Based on the SEC Guidance and the rules and regulations described above, the SEC has launched various cyber-related enforcement actions. The

- In an action brought under Regulation S-P, *In the Matter of LPL Financial Corporation* (LPL), the SEC targeted a registered broker-dealer

  LPL failed to implement adequate controls, including some security measures, which left

  make unauthorized trades in various customer

representatives maintain antivirus software on their computers, which the registered representatives used to access customer

trading platform. In addition, Commonwealth did not have procedures in place to adequately monitor and review its registered representatives' computer security measures and their implementation. In November 2008, through the use of a computer virus, an unauthorized party obtained the log-in

- One example of this engagement has been the regular treatment of the subject in the organization's Regulatory and Examination Priorities Letter since 2007.
-
- Also, in 2010 and 2011, FINRA conducted

  and business models to determine and assess the means by which registered

  technology and cyber risks.
-
- Another important activity in this same vein was the June 2001 FINRA survey of

  light on relevant industry information technology and cybersecurity practices

  protection and market integrity.[51]
-
- (Sweep) focused on the types of threats

  to managing these threats. In this examination, FINRA sent an information

  including large investment banks,

  frequency traders and independent dealers.
-
- Report), which drew upon a variety of

  interviews with other organizations involved in cybersecurity, previous FINRA work on cybersecurity and publicly

  cybersecurity programs:

- cybersecurity governance and risk management;
- cybersecurity risk assessment;
- technical controls;
- incident response planning;
- vendor management;
-
- cyber intelligence and information sharing; and
- cyber insurance.[52]

sub-categories that provided the basis for the

analyzed in the FINRA Report and summarized in Section V (A) of this Research Report.

Note that, rather than covering all cybersecurity topics or providing exhaustive guidance on each cybersecurity issue discussed, the FINRA Report

Against this background of investigation, evaluation and assessment, FINRA has proceeded with various enforcement matters. The following

reproduced verbatim from the FINRA Report. They are illustrative of present and likely future enforcement scenarios.

- In one instance where FINRA took enforcement

  for higher-risk foreign customers who engaged in a pattern of fraudulent trading through the

Justice (DOJ) Criminal Division is responsible for implementing the Department's national strategies in combating computer and intellectual property

The Gameover Zeus botnet was a global network of somewhere between 500,000 and one million infected victim computers which were used to steal millions of dollars

also a common distribution mechanism for Cryptolocker a form of malicious software

researchers estimate that, as of April 2014, Cryptolocker had infected more than 234,000 computers...

In any event, the sort of collaboration that we achieved in the Gameover Zeus operation was

at the Legal Symposium on cybercrime on this campus, I announced that the department

Division's plan to work more closely with the private sector and federal agencies to address

for the Division's cybersecurity work, which is the new Cybersecurity Unit in CCIPS ... In creating the Unit, we hope to use the lessons that CCIPS has learned and the skills that its prosecutors have gained from investigating and disrupting cybercrime to create actionable guidance and to support public- and private-

65

consumers who use or visit its commercial Web site or online service and the categories of third-party persons or entities with whom the operator may share that personally

In addition, the statute states the following:

- suit against FileFax Inc., a document storage company, for allegedly exposing thousands of patient medical records containing social security numbers and other personal information. The records were those of patients of Suburban Lung Associates, which contracted with FileFax to maintain and destroy them. The suit alleges FileFax failed to provide safe and secure collection, retention, storage and destruction of the records, citing one instance where FileFax disposed of records in a publicly accessible unlocked garbage dumpster outside its facility.
- Vermont Attorney General William Sorrell

  San Francisco, resolving allegations the hotel failed to notify consumers of a security breach without unreasonable delay. The hotel had

  unauthorized charges on their credit cards, but did not send notice of a breach to residents until six months later.[75]

The publication also reports on the progress of state adoptions of new cyber-related laws, whose enactment will arguably greatly strengthen the

the public interest in this area.[76]

One potential enforcement matter that illustrates how major cases evolve concerns an investigation

approach and the adroit (and interestingly

attorneys general, as revealed in the following article excerpt from *The Wall Street Journal*. The

which two state attorneys general may be on the verge of initiating enforcement action in behalf of

> At least two state attorneys general are investigating J.P. Morgan Chase & Co. for its handling of a cyberattack this summer that compromised customer contact information of about 76 million households and 7 million small businesses, according to people familiar with the matter.
>
> George Jepsen has been in contact with the bank regarding the cyberattack since the bank's disclosure earlier this year, a spokeswoman for the attorney general said. She declined to provide further detail, saying it was a pending matter.
>
> Illinois Attorney General Lisa Madigan is also looking into the breach. In a statement Friday, Ms. Madigan said that the cyberattack is
>
> it shows how vulnerable U.S. institutions and their databases are.
>
> their money and personal information, but by failing to be forthcoming, they have lost their
>
> Ms. Madigan said the cyberattack demands
>
> be shared with the public, since consumers' [77]

In general, a review of the various laws and enforcement activities at the state level make clear that the state law patchwork is obviously

but the larger national picture of cybersecurity enforcement is not one of uniformity at present.

One important area of note in the cybersecurity arena is the challenge of private litigation against companies for failure to provide for proper cybersecurity governance. These cases are likely to be based on one or more of the following legal theories:

- Breach of contract;
-

- Waste of corporate assets;
-

system in our U.S. stores. On December 15, we removed the malware from virtually all registers in our U.S. stores. Payment card data used in transactions made by 56 additional guests in the period between December 16 and December 17 was stolen prior to our disabling malware on one additional register that was disconnected from our system when we completed the initial malware removal on December 15. In addition, the intruder stole certain guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals. Our investigation of the matter is ongoing, and we are

responsible parties.

Expenses Incurred and Amounts Accrued

In the fourth quarter of 2013, we recorded $61 million of pretax Data Breach-related expenses, and expected insurance proceeds of $44 million, for net expenses of $17 million ($11 million after tax), or $0.02 per diluted share. These expenses were included in our Consolidated Statements of Operations as Selling, General and Administrative

investigation of the Data Breach is ongoing, and we

the responsible parties.

In addition to the above expenses, we believe it is probable that the payment card networks will make claims against us. The ultimate amount of these claims will likely include amounts for incremental counterfeit fraud losses and non-ordinary course operating expenses (such as card reissuance costs) that the payment card networks assert they or their issuing banks have incurred.

courts in the U.S. and Canada, and other claims may be asserted against us on behalf of customers, payment card brands, payment card issuing banks, shareholders or others seeking damages or other related relief, allegedly arising from the Data Breach. Furthermore, several state and federal agencies, including State Attorneys General, are investigating events related to the Data Breach, including how it occurred, its consequences and our responses. We are cooperating in the governmental investigations, and we may be

(United States District Court, District of New Jersey)

, Case No. 2:14-cv-01234-SRC-CLW for (1) Breach of Fiduciary Duty, (2) Waste of Corporate Assets and (3) Unjust Enrichment)

1.

on behalf of nominal defendant Wyndham

and members of its Board of Directors

0%ÐD5ªÂ Ä,ç–6ïÎÝíÙ,È•V–6ì^ @pˆ Ìp–À Éjþ..ÀÿpWŽÀÀ Œõ`F³V@LPR€Q ðð@ € pÞÀÃÀ P P ?@ ` p À P ÿHUWDLP?ÀP

comment letter demanding that WWC timely

6. The defendants' failures to implement appropriate internal controls at WWC designed to detect and prevent repetitive data breaches have severely damaged WWC. The Company is currently a defendant

deception-based violations of section 5 of

The FTC Action poses the risk of tens of millions of dollars in further damages to

> recent legislative and regulatory initiatives, the scope of the Act is now even broader than ever before, imposing its disclosure requirements and other procedures on many organizations that serve as investment advisers to private

[88]

In an era of increasingly stringent cybersecurity consciousness, as well as government enforcement

must be prepared to set properly high levels of cybersecurity governance. Similarly, private equity

same advice. These points are underscored by the following predictions of a prominent legal practitioner in the area:

> As we look ahead to 2015 and 2016, there are three major issues impacting the private equity market: (1) increased regulatory oversight regarding the activities of private
>
> part of the limited partner investors that invest ... and (3) a rebalance of negotiating leverage between the general partners that manage the fund and the limited partners.[89e]

LEGAL DUTIES AND LIABILITIES FOR CYBERSECURITY GOVERNANCE IMPOSED DIRECTLY ON THE BOARD OF DIRECTORS AND OFFICERS

Directors and O f cers

under the law, but it cannot act for itself. It must act through people, and these people take on

investment bankers and others (both inside and outside the corporation). Moreover, the board of directors plays a primary, indeed a central, role in the governance of the corporation. For example, Delaware General Corporation Law (DGCL) § 141 (a) provides as follows:

> organized under this chapter shall be managed by or under the direction of a board of directors ....[91]

corporate law certain standards of conduct and liability for how directors manage the corporation.

power and authority from the directors include

duties are owed to the corporation and the shareholders[92]. This means that usually only the corporation (including through a representative) or the shareholders may sue the directors and

these duties.[93]
concept sends the following message:

> Carry out your assigned duties properly, in the corporation's and the shareholders' best interests, and if you do not do so, you may be sued and held personally liable for economic injuries that come to the corporation or the shareholders because of that failure of duty.

law has generally been structured into two major

as well as certain additional duties, notably for

(monitoring).[94]

fundamental requirement and guide in corporate law whose rationale is clearly self-evident. More

American Law Institute (ALI) Principles of Corporate Governance, Section 4.01(a) requires that directors carry out their work for the corporation:

> in good faith, in a manner that he or she reasonably believes to be in the best interests of the corporation, and with the care that an ordinarily prudent person would reasonably be expected to exercise in a like position and under similar circumstances.[95]

Furthermore, directors must meet this standard at a minimum, meaning that they have no legal

of winning in a lawsuit like this against the

Another exception to, or limitation on, limited

This legal concept is completely separate and apart

concept says the following:

> Just because you work for a corporation, you don't have limited liability in every situation. If you participate directly or actively in an illegal act (including supervising others in the commission of one), you will be held

- *August 2014*

  This Resolution addresses cybersecurity issues that are critical to the national and economic security of the United States

  sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and to the data and systems to be protected.

- *August 2013*

  This Resolution condemns intrusions into computer systems and networks utilized

  state, and other governmental bodies to

  intrusions.

- cybersecurity principles developed by the Cybersecurity Legal Task Force. The Resolution reads as follows:

  > RESOLVED, That the American Bar Association urges the Executive and Legislative branches to consider the following guiding principles throughout the decision-making process when making U.S. policy determinations to improve cybersecurity for the U.S. public and private sectors:
  >
  > - : Public-private frameworks are essential to successfully protect United States assets, infrastructure, and economic interests from cybersecurity attacks.
  > - : Robust information sharing and collaboration between government agencies and private industry are necessary to manage global cyber risks.
  > - : Legal and policy environments must be modernized to stay ahead of or, at a minimum, keep pace with technological advancements.
  > - : Privacy and civil liberties must remain a priority when developing cybersecurity law and policy.
  > - : Training, education, and workforce development of government and 18 corporate senior leadership, technical operators, and lawyers require adequate investment and resourcing in cybersecurity to be successful.[118]

- *August 2012*

  The ABA House of Delegates amends the black letter and Comments to Model Rules 1.0, 1.6, and 4.4, and the Comments to Model Rules 1.1

Association of Corporate Directors (NACD) has produced a guidance document entitled *Cyber*

- Firms should implement technical

  hardware that stores and processes data, as well as the data itself.

- Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cybersecurity incidents.

- Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management.

- **Sta f Training**

  Firms should provide cybersecurity

- Firms should use cyber threat intelligence to improve their ability to identify, detect and respond to cybersecurity threats.

- Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes.

-
    - Have an Actionable Plan in Place Before an Intrusion Occurs
    - Have Appropriate Technology and Services in Place Before An Intrusion Occurs
    - Have Appropriate Authorization in Place to Permit Network Monitoring
    - Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident
    - Ensure Organization Policies Align with Your Cyber Incident Response Plan
    - Engage with Law Enforcement Before an Incident
    - Establish Relationships with Cyber Information Sharing Organizations
- Responding to a Computer Intrusion: Executing Your Incident Response Plan
    - Step 1: Make an Initial Assessment
    - Step 2: Implement Measures to Minimize Continuing Damage
    - Step 3: Record and Collect Information
    - Step 4: Notify
- What Not to Do Following a Cyber Incident
    - Do Not Use the Compromised System to Communicate
    - Do Not Hack Into or Damage Another Network

This very thorough set of guidelines concludes with [130] that is extremely helpful in and of itself.

The practical advice contained in this section is the product of many of the sources used in this Research Paper. The advice is not exhaustive, but it is meant to be comprehensive by serving as the core of a cybersecurity corporate governance program under the supervision of the corporation's board of directors:

- First, review all the best practices standards and guidelines discussed above and compare your own company's program to them, both at a distance and in detail;
- Consider retaining a consultant on cybersecurity governance (remember the

  and an IT expert). For most companies, this

  certainly compares favorably to the direct and secondary costs of a cyberattack;
- The process of designing or improving a cybersecurity governance program should

  (board of directors and relevant board

  counsel and perhaps the most substantial shareholders);
- Obtaining buy-in for acceptance requires open endorsement at the highest levels of the company, with those persons participating in presentations, training sessions and other means of clarifying that the program is an integral part of the company's corporate governance framework;
- Remember that constant evaluation and

  fundamental requirement, which is a universal best practice.

As emphasized in Section II (E) of this Research Report, the role of legal counsel is crucial in cybersecurity governance. Essentially, they play a special, exclusive role in guiding the board of

entire governance process, while bringing to bear a thorough knowledge of the law and the legal

in that process. The following guidance is the product of a 10-point agenda developed by Harriet

study conducted by the Maurer School of Law at Indiana University. It should be borne in mind by legal counsel in performing these duties.

1. **Ful f ll Fiduciary Duty of Board and**
   Prove the company's directors and management met their duty to safeguard the company's stock price and assets. (32% of

END NOTES

[1] *See, e.g.* Pedro J. Martinez-Fraga,
(Cambridge University Press 2014), tracing the contours of US doctrinal developments concerning international commercial arbitration.

[2] *See, e.g.* https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf.

[3] *Ponemon Institute Research Report*, May 2015, available at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF.

[4] *Id.*

[5] *Id.* at 1-3.

[6] *Id.* at 1-3.

[7] *See*

[25] *U.S. v. Yelp Inc.* *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3066/yelp-inc.; *U.S. v. TinyCo, Inc.* *available at* https://www.ftc.gov/enforcement/cases-proceedings/132-3209/tinyco-inc.

[26]

and Cybersecurity Roundtable, Sidley Austin LLP, March 3, 2015, available at statements/671241/150303sidleyaustin.pdf.

[27] *See generally* *Securities Regulation*

[28] 77a

[29] 15 U.S.C. 78a et seq.

[30] 15 U.S.C. –77bbbb.

[31] 15 U.S.C. –

[50] *See* https://mailhost.wcl.american.edu/exchange/wallace/Inbox/FINRA%20Guidelines.EML/1_multipart_xF8FF_2_FINRA_Report%20on%20Cybersecurity%20Practices.pdf/C58EA28C-18C0-4a97-9AF2-036E93DDAFB3/FINRA_Report%20on%20Cybersecurity%20Practices.pdf?attach=1.

[51] *Id.*

[52]

Standards and Technology (NIST), available at http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[53] FINRA Report, page 5.

[54]

data/354950/000035495015000008/hd-212015x10xk.htm#s301FBDE93E5897A646E64F74E64E6BC1.

79

[104] *See, e.g.*, Del. Gen. Corp. Law Sec. 102(b) (7); Virginia Corporations Code Sec. 13.1-690.

[105] *See, e.g.*

[106] *See, e.g.*, Del. Gen. Corp. Law Sec 145; Model Bus. Corp. Act Secs. 8.50-8.59; Cal. Corp. Code Sec. 317.

[107] *See, e.g.*, Melvin Aron Eisenberg & James D. Cox, Corporations and Other Business Organizations 490-92 (2011).

[108] *Stone*, 911 A.2d at 371

[109] Securities Act of 1933, Section 11.

[110] People ex rel. Madigan v. Tang, 346 Ill. App. 3d 277 (2004).

[111] *Id.* at 289.

[112] IU/Hanover article

[113] *See*, ABA Legal Task Force website, available at .

[114] http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/aba_cybersecurity_res_and_report.authcheckdam.pdf.

[115] *Id.*

[116] *Id.*

[117] *Cybersecurity: Boardroom Implications*, 2014, NACD, available at https://www.nacdonline.org/applications/secure/?FileID=88578.

[118] *Id.* at 6-7.

[119] *Cyber-Risk Oversight Handbook*, NACDJune 10, 2014, available at https://www.nacdonline.org/Cyber.

[120] *Id.* at 3.

[121]

ABOUT THE AUTHORS

PERRY E. WALLACE

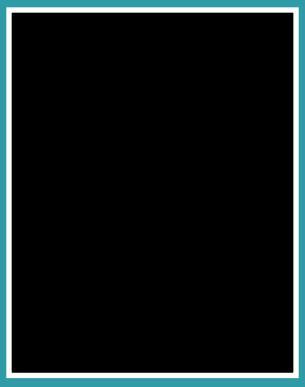
Professor Perry E. Wallace received his undergraduate degree in electrical engineering and engineering mathematics from the Vanderbilt University School of Engineering. He received his law degree from Columbia University, where he was awarded the Charles Evans Hughes Fellowship. He is a tenured Professor of Law at the Washington College of Law of the American University, where he teaches corporate, environmental and international law.

Professor Wallace was for several years a senior trial attorney at the United States Department of Justice, handling cases involving environmental and natural resources law. He has also served as a securities and commercial arbitrator. Professor Wallace has served on numerous boards, commissions and councils over the years, including the U.S. Environmental Protection Agency's National Advisory Council for Environmental Policy and Technology, the Environmental Working Group and the Academic Council of the Institute for Transnational Arbitration.

Dr. Richard Schroth is a trusted private advisor and thought leader to business around the globe. He is Executive Director of The Kogod Cybersecurity Governance Center at American University and an Executive in Residence. Honored as one of the Top 25 Consultants in the World by Consulting Magazine and his peers, Richard is the Managing Director of the Newport Board Group's Global Technology Strategy, Innovation and Cyber Practice and the Axon Global Cyber Alliance, where he actively leads world-class teams of cyber professionals and board level advisors seeking to minimize the serious nature of cyber risk.

Dr. Schroth is energetically engaged in the cutting-edge of global private sector cyber initiatives including areas of M&A cyber diligence, board policies for cyber risk and advanced cyber business

WILLIAM DELONE



William DeLone is an Eminent Professor of Information Technology at the Kogod School of Business at American University and Executive Director of the Kogod Cybersecurity Governance Center. Professor DeLone earned a B.S. in mathematics from Villanova University; an M.S. in industrial administration from Carnegie-Mellon University; and a Ph.D. in Computers and Information Systems from the University of California, Los Angeles. His dissertation studied the successful use of computers and information systems by small businesses. He has served as Acting Dean, Senior Associate Dean, and Chair of the Department of Information Technology. He also served as Chair of American University's Strategic Planning Steering Committee.

Professor DeLone's primary areas of research include the assessment of information systems'

public value and the management of global software development Professor DeLone has been published in the top information systems journals. Professor DeLone has lectured and consulted on information systems at universities in London, Paris, Rome, Venice, Warsaw, Galway, Singapore, Kuwait, Leipzig & Saarbrucken in Germany, and Guatemala.

ACKNOWLEDGEMENTS

The Kogod Cybersecurity Center would like to

ADVISORY COMMITTEE

,
Lockton

,
FINRA

,
Dean

,
US Department of Commerce

,
Greater Washington Board of Trade

(liaison),
NIST

,
AIG

Bruce Ho f meister,
Marriott International

,
Discovery Communications

,
Association of Capital Growth

,
Protiviti

,
Axon Global Services

,
The Messina Group

,
Vectra Networks

,
U.S. Secret Service

,
American University

,
Senior Fellow

,
Executive in Residence

,
Raytheon

KCGC LEADERSHIP

,
Executive Director

,
Executive Director

,
Director of Center Operations

,
Faculty Research Director

THIS PUBLICATION IS SPONSORED BY

A