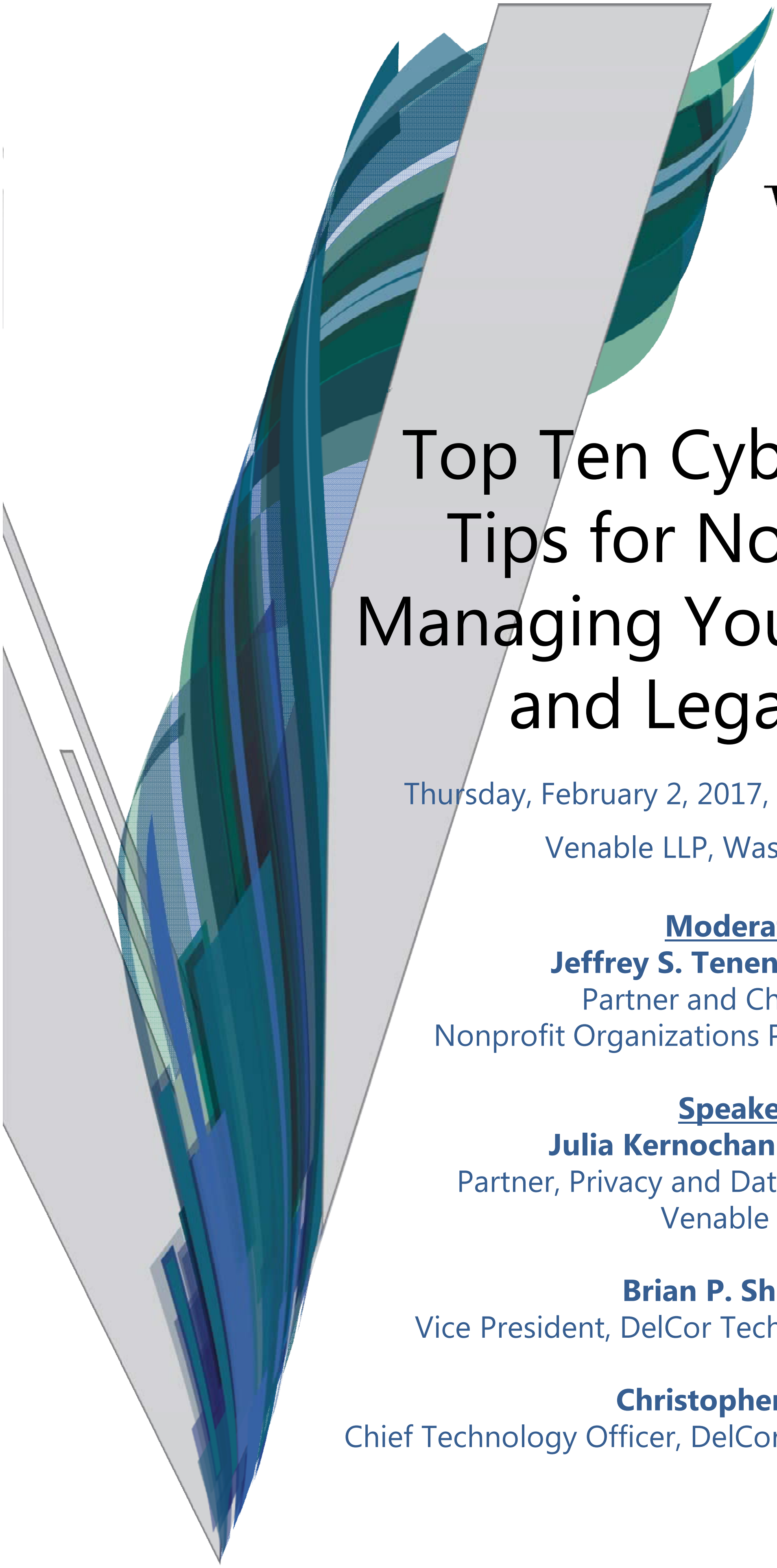


VENABLE

Top Ten Cybersecurity Tips for Nonprofits: Managing Your Technical and Legal Risks

Thursday, February 2, 2017, 12:30 pm – 2:00 pm ET

Venable LLP, Washington, DC

Moderator
Jeffrey S. Tenenbaum, Esq.
Partner and Chair of the
Nonprofit Organizations Practice, Venable LLP

Speakers
Julia Kernochan Tama, Esq.
Partner, Privacy and Data Security Practice,
Venable LLP

Brian P. Sheehan
Vice President, DelCor Technology Solutions, Inc.

Christopher Ecker
Chief Technology Officer, DelCor Technology Solutions, Inc.

Presentation

VENABLE

Top Ten Cybersecurity Tips for Nonprofits: Managing Your Technical and Legal Risks

Thursday, February 2, 2017, 12:30 pm – 2:00 pm ET

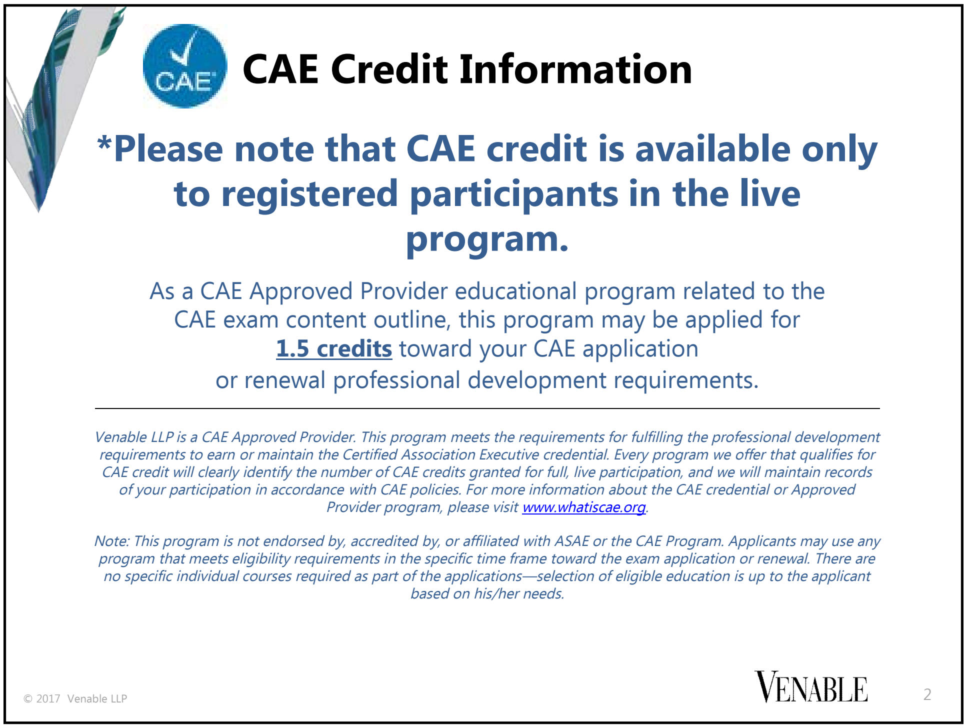
Venable LLP, Washington, DC

Moderator
Jeffrey S. Tenenbaum, Esq.
Partner and Chair of the Nonprofit Organizations Practice, Venable LLP

Speakers
Julia Kernochan Tama, Esq.
Partner, Privacy and Data Security Practice, Venable LLP

Brian P. Sheehan
Vice President, DelCor Technology Solutions, Inc.

Christopher Ecker
Chief Technology Officer, DelCor Technology Solutions, Inc.



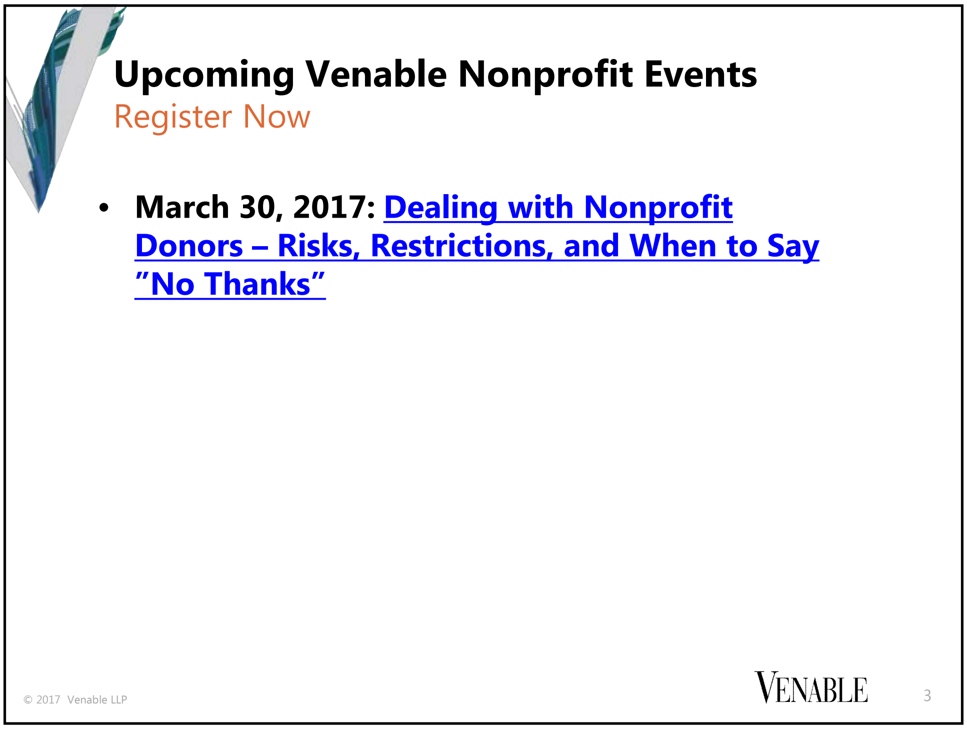
CAE Credit Information

***Please note that CAE credit is available only to registered participants in the live program.**

As a CAE Approved Provider educational program related to the CAE exam content outline, this program may be applied for **1.5 credits** toward your CAE application or renewal professional development requirements.

Venable LLP is a CAE Approved Provider. This program meets the requirements for fulfilling the professional development requirements to earn or maintain the Certified Association Executive credential. Every program we offer that qualifies for CAE credit will clearly identify the number of CAE credits granted for full, live participation, and we will maintain records of your participation in accordance with CAE policies. For more information about the CAE credential or Approved Provider program, please visit www.whatiscae.org.

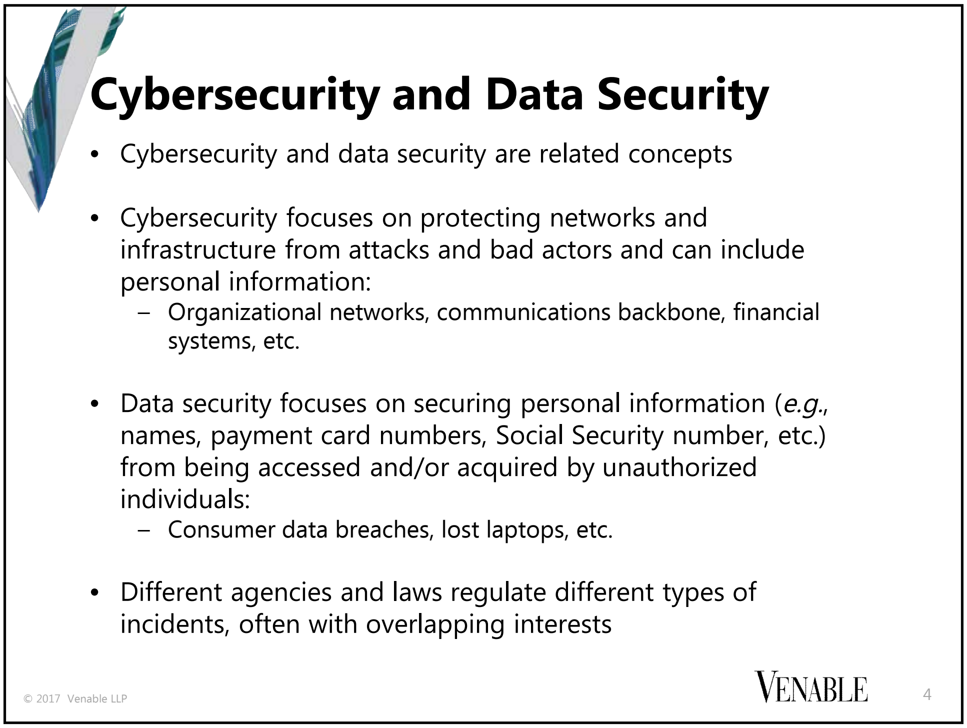
Note: This program is not endorsed by, accredited by, or affiliated with ASAE or the CAE Program. Applicants may use any program that meets eligibility requirements in the specific time frame toward the exam application or renewal. There are no specific individual courses required as part of the applications—selection of eligible education is up to the applicant based on his/her needs.



Upcoming Venable Nonprofit Events

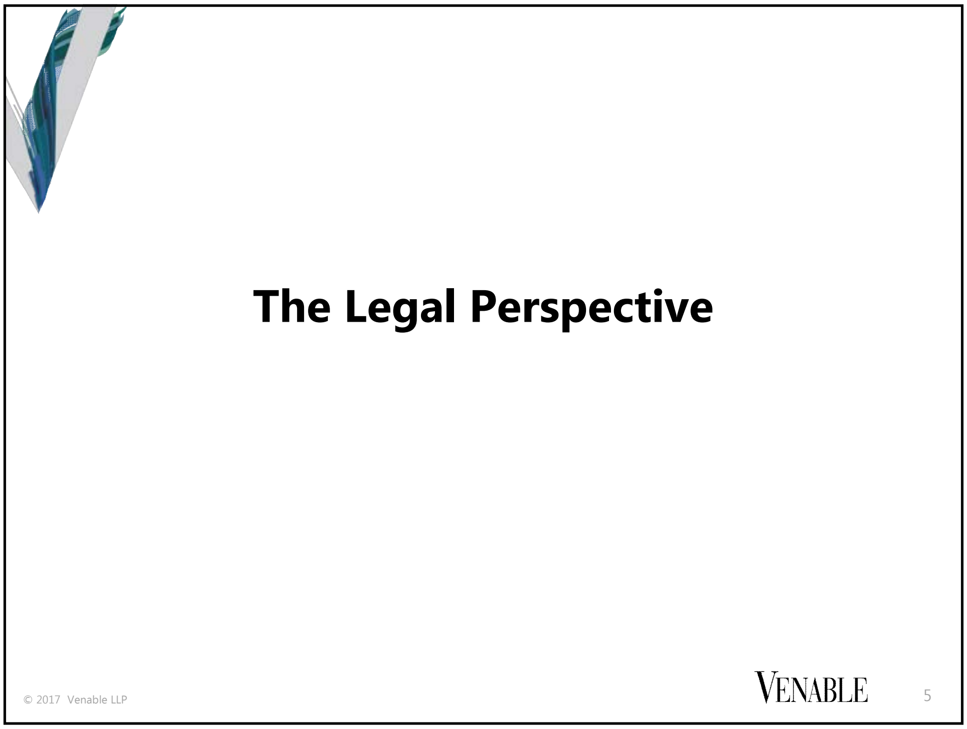
Register Now

- **March 30, 2017: Dealing with Nonprofit Donors – Risks, Restrictions, and When to Say ”No Thanks”**

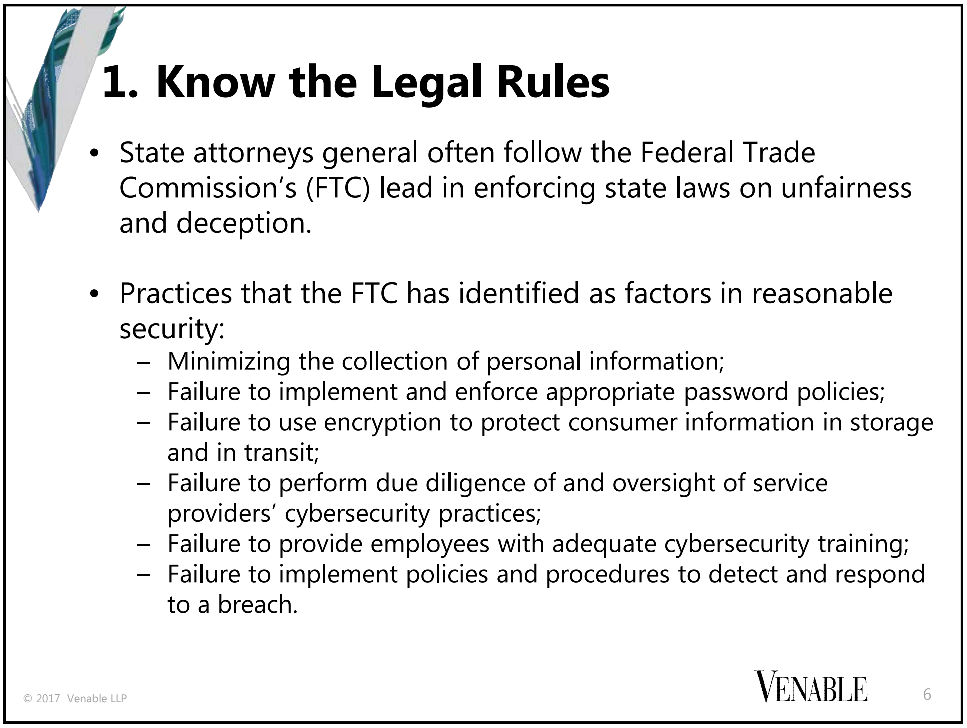


Cybersecurity and Data Security

- Cybersecurity and data security are related concepts
- Cybersecurity focuses on protecting networks and infrastructure from attacks and bad actors and can include personal information:
  - Organizational networks, communications backbone, financial systems, etc.
- Data security focuses on securing personal information (*e.g.*, names, payment card numbers, Social Security number, etc.) from being accessed and/or acquired by unauthorized individuals:
  - Consumer data breaches, lost laptops, etc.
- Different agencies and laws regulate different types of incidents, often with overlapping interests



The Legal Perspective



1. Know the Legal Rules

- State attorneys general often follow the Federal Trade Commission’s (FTC) lead in enforcing state laws on unfairness and deception.
- Practices that the FTC has identified as factors in reasonable security:
  - Minimizing the collection of personal information;
  - Failure to implement and enforce appropriate password policies;
  - Failure to use encryption to protect consumer information in storage and in transit;
  - Failure to perform due diligence of and oversight of service providers’ cybersecurity practices;
  - Failure to provide employees with adequate cybersecurity training;
  - Failure to implement policies and procedures to detect and respond to a breach.

1. Know the Legal Rules

- State Data Security Laws:
  - Nine states require that organizations implement sufficient policies and procedures to maintain reasonable data security
  - Typically apply based on individuals' residence, not the entity's location
  - AR, CA, FL, CT, IN, MD, OR, TX, UT

- Massachusetts Standards for the Protection of Personal Information:
  - MA has implemented more detailed data security requirements that apply to associations and other legal entities
  - Requires a written comprehensive information security program, with specific components and technical requirements

- Data Disposal:
  - Approximately 30 states impose legal obligations on organizations to properly dispose of records that contain personal, financial, or health information

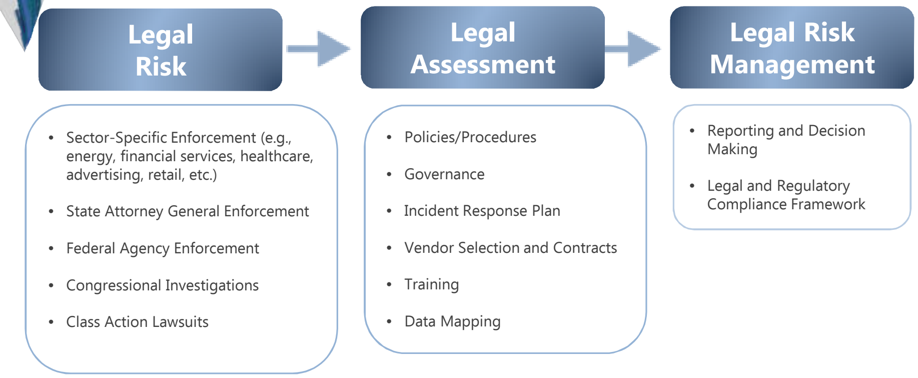
1. Know the Legal Rules

- Payment Card Industry Data Security Standards (PCI DSS):
  - Regularly updated security standards created by the credit card industry
  - Practices and policies to protect accountholder data

- Implementation:
  - Compliance steps depend on card processing volume
  - Qualified Security Assessors (QSAs) can assist
  - Information security policy is required
  - Service providers should be PCI DSS compliant

- Enforcement:
  - Credit card brands require merchant banks to enforce compliance by their clients
    - o Fines imposed on banks can be passed on to organizations
  - States have enacted statutory requirements similar to PCI DSS

2. Assess Your Risks



Legal Risk

- Sector-Specific Enforcement (e.g., energy, financial services, healthcare, advertising, retail, etc.)
- State Attorney General Enforcement
- Federal Agency Enforcement
- Congressional Investigations
- Class Action Lawsuits

Legal Assessment

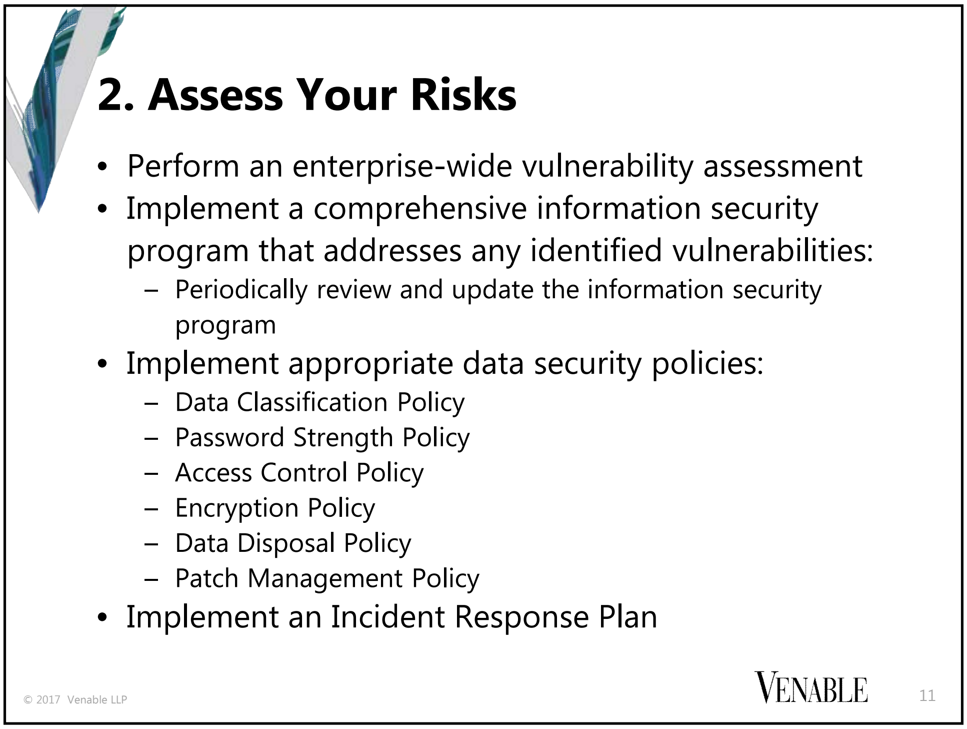
- Policies/Procedures
- Governance
- Incident Response Plan
- Vendor Selection and Contracts
- Training
- Data Mapping

Legal Risk Management

- Reporting and Decision Making
- Legal and Regulatory Compliance Framework

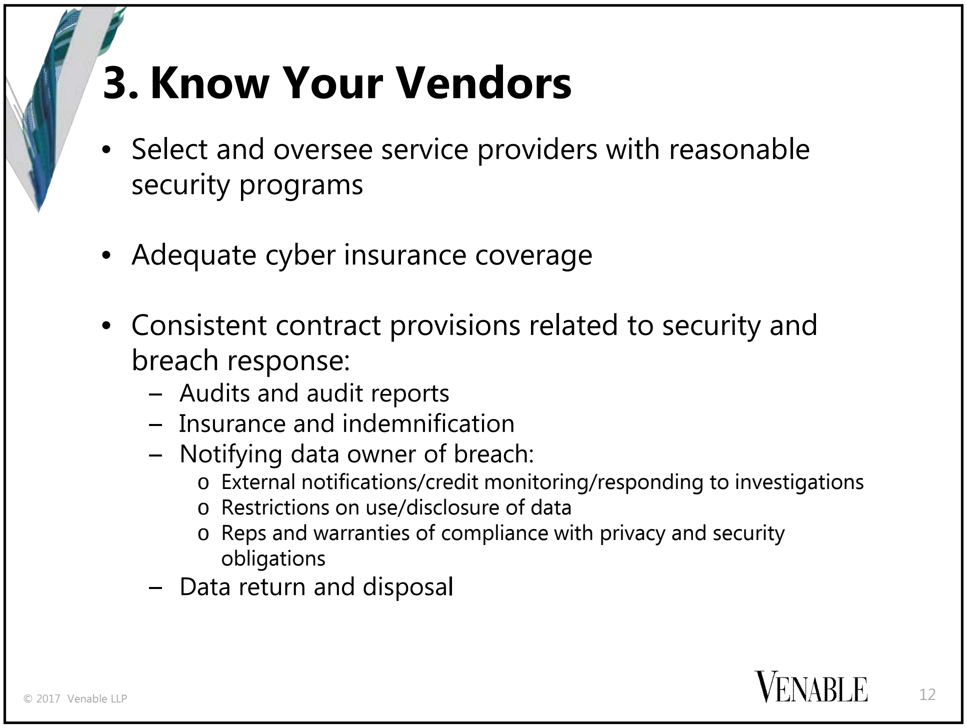
2. Assess Your Risks

- Security program should be proportional to:
  - Data handled
  - Size and nature of organization
- Administration began to focus on cybersecurity in earnest beginning in 2013:
  - Executive Order 13636 directed the National Institute of Standards and Technology (NIST) to develop a baseline cybersecurity framework
- NIST released the Cybersecurity Framework in February 2014:
  - **Voluntary** methodology and process for assessing and reducing cybersecurity risks in critical infrastructure sectors
  - Framework is a "living document," and NIST continues to gather feedback regarding how to improve it over time
  - NIST reports good uptake of the Framework, including by FINRA and the Conference of State Bank Supervisors
  - **Updated draft v. 1.1 released for comment on January 10, 2017**



2. Assess Your Risks

- Perform an enterprise-wide vulnerability assessment
- Implement a comprehensive information security program that addresses any identified vulnerabilities:
  - Periodically review and update the information security program
- Implement appropriate data security policies:
  - Data Classification Policy
  - Password Strength Policy
  - Access Control Policy
  - Encryption Policy
  - Data Disposal Policy
  - Patch Management Policy
- Implement an Incident Response Plan

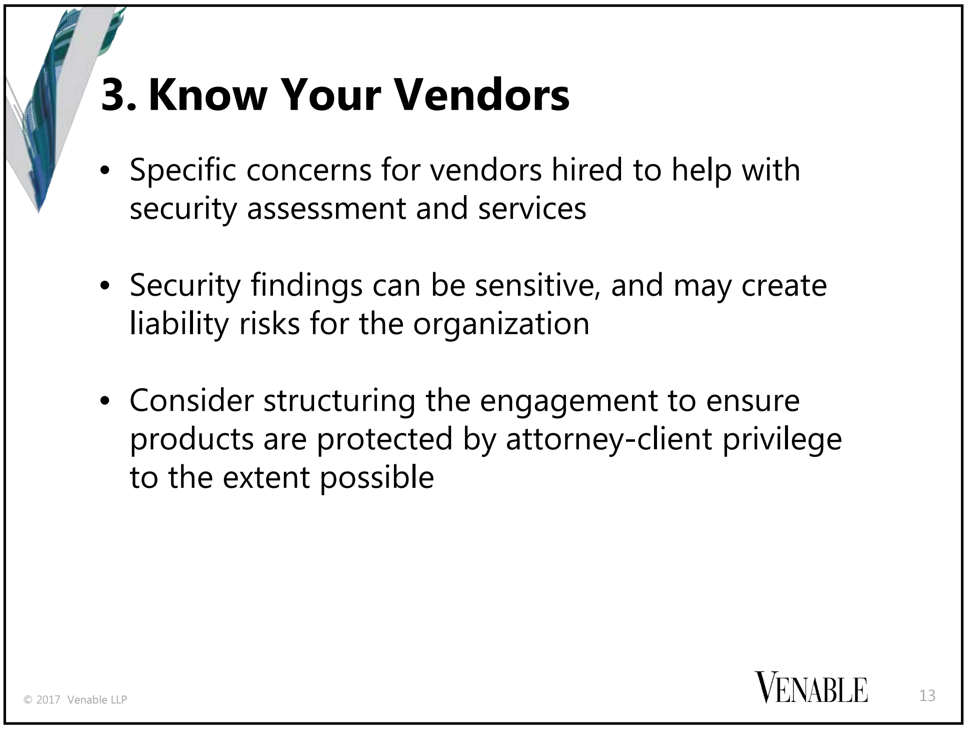


3. Know Your Vendors

- Select and oversee service providers with reasonable security programs

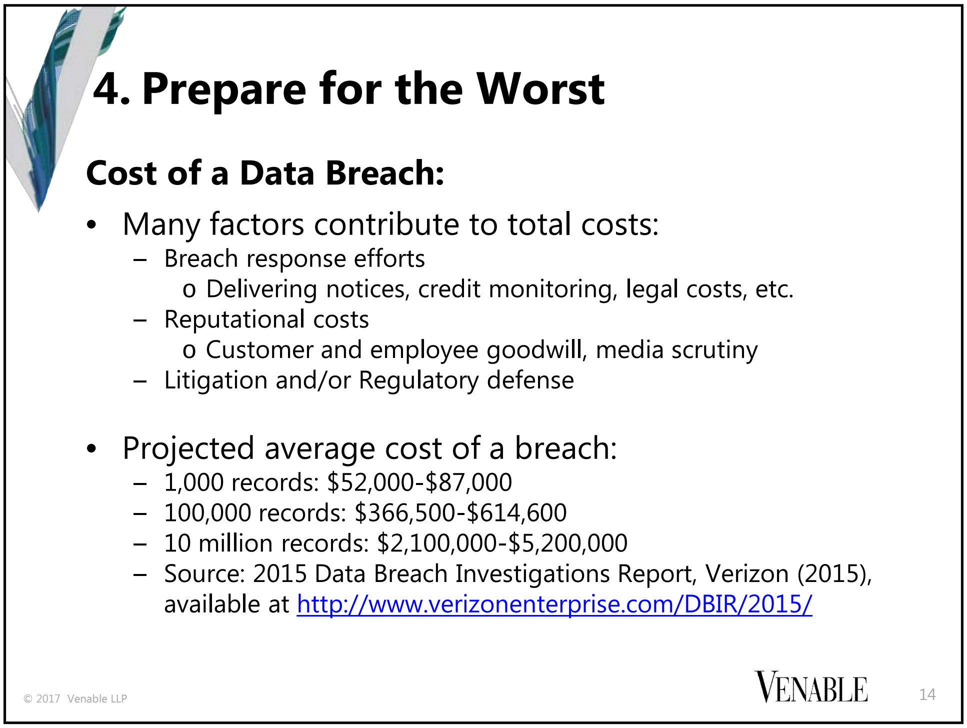
- Adequate cyber insurance coverage

- Consistent contract provisions related to security and breach response:
  - Audits and audit reports
  - Insurance and indemnification
  - Notifying data owner of breach:
    - External notifications/credit monitoring/responding to investigations
    - Restrictions on use/disclosure of data
    - Reps and warranties of compliance with privacy and security obligations
  - Data return and disposal



3. Know Your Vendors

- Specific concerns for vendors hired to help with security assessment and services
- Security findings can be sensitive, and may create liability risks for the organization
- Consider structuring the engagement to ensure products are protected by attorney-client privilege to the extent possible



4. Prepare for the Worst

Cost of a Data Breach:

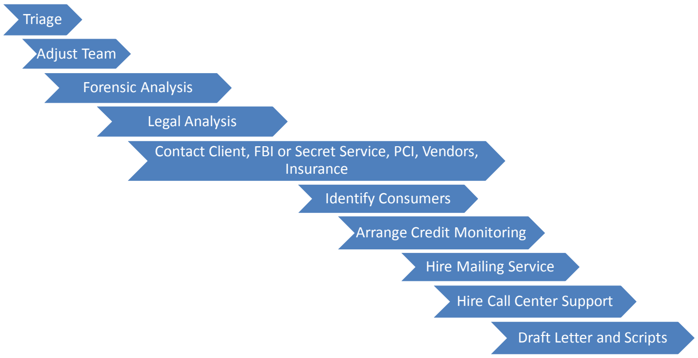
- Many factors contribute to total costs:
  - Breach response efforts
    - o Delivering notices, credit monitoring, legal costs, etc.
  - Reputational costs
    - o Customer and employee goodwill, media scrutiny
  - Litigation and/or Regulatory defense
- Projected average cost of a breach:
  - 1,000 records: $52,000-$87,000
  - 100,000 records: $366,500-$614,600
  - 10 million records: $2,100,000-$5,200,000
  - Source: 2015 Data Breach Investigations Report, Verizon (2015), available at http://www.verizonenterprise.com/DBIR/2015/

4. Prepare for the Worst

- An effective incident response plan will facilitate:
  - Prompt detection, investigation, recovery (more on this later);
  - Notification of and cooperation with law enforcement officials, if deemed necessary;
  - Notification to external parties affected by the incident, if any, such as customers, associates, or credit card companies;
  - Notification to cyber insurance provider, if necessary;
  - Notification to affected individuals, if required;
  - Notification to state or federal regulatory agencies, if required;
  - Review of security policies and procedures to prevent a reoccurrence

4. Prepare for the Worst

Breach Response Timeline: “Sprinting a Marathon”



Triage

Adjust Team

Forensic Analysis

Legal Analysis

Contact Client, FBI or Secret Service, PCI, Vendors, Insurance

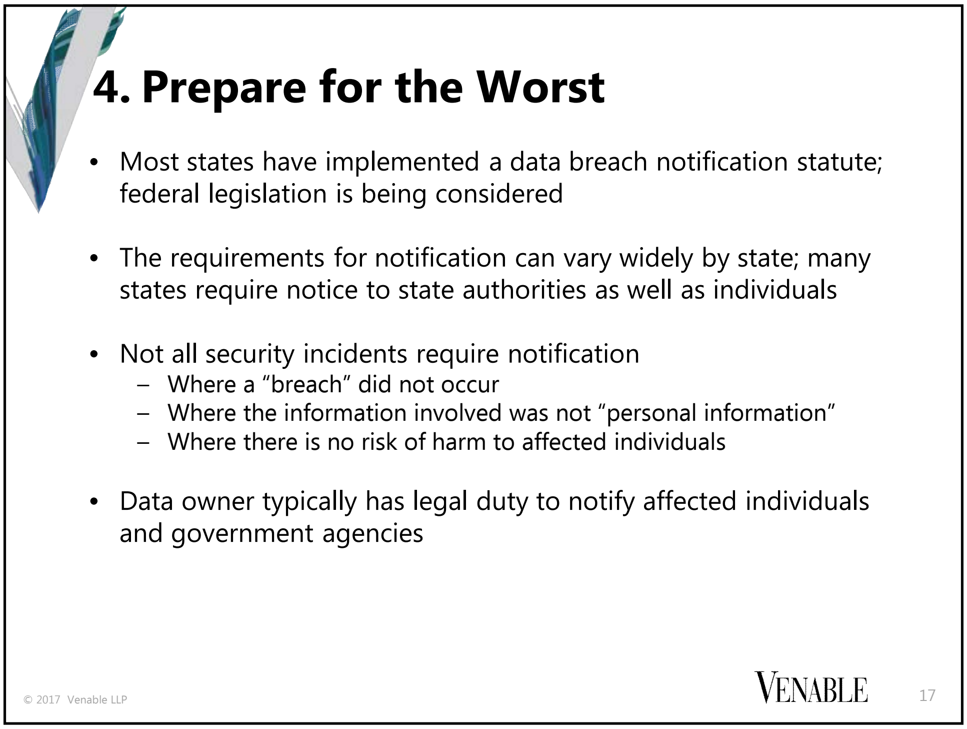
Identify Consumers

Arrange Credit Monitoring

Hire Mailing Service

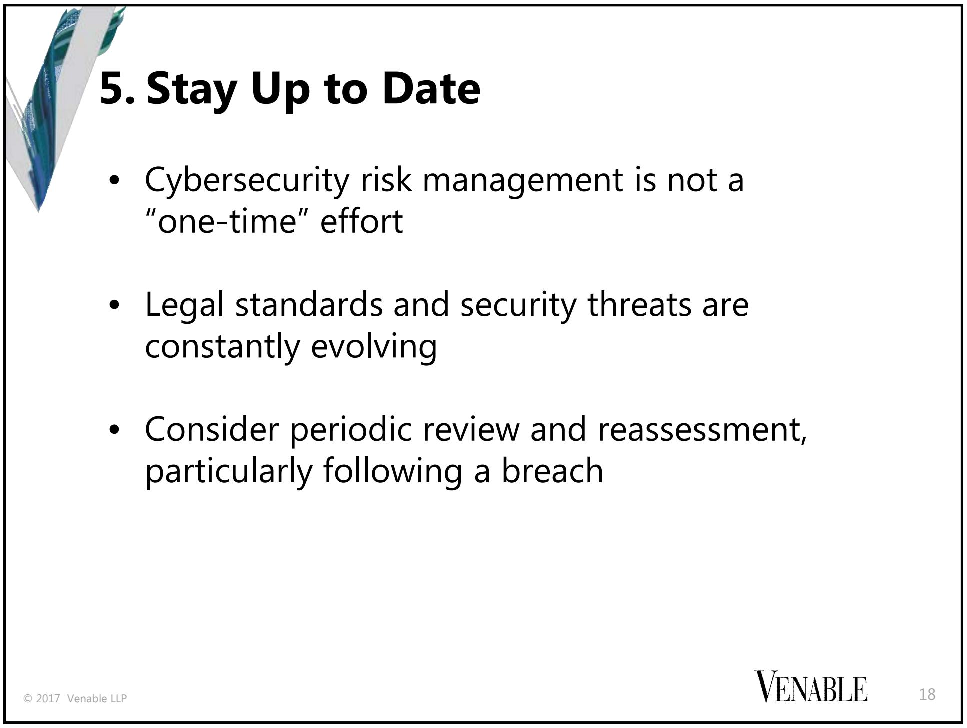
Hire Call Center Support

Draft Letter and Scripts



4. Prepare for the Worst

- Most states have implemented a data breach notification statute; federal legislation is being considered
- The requirements for notification can vary widely by state; many states require notice to state authorities as well as individuals
- Not all security incidents require notification
  - Where a “breach” did not occur
  - Where the information involved was not “personal information”
  - Where there is no risk of harm to affected individuals
- Data owner typically has legal duty to notify affected individuals and government agencies

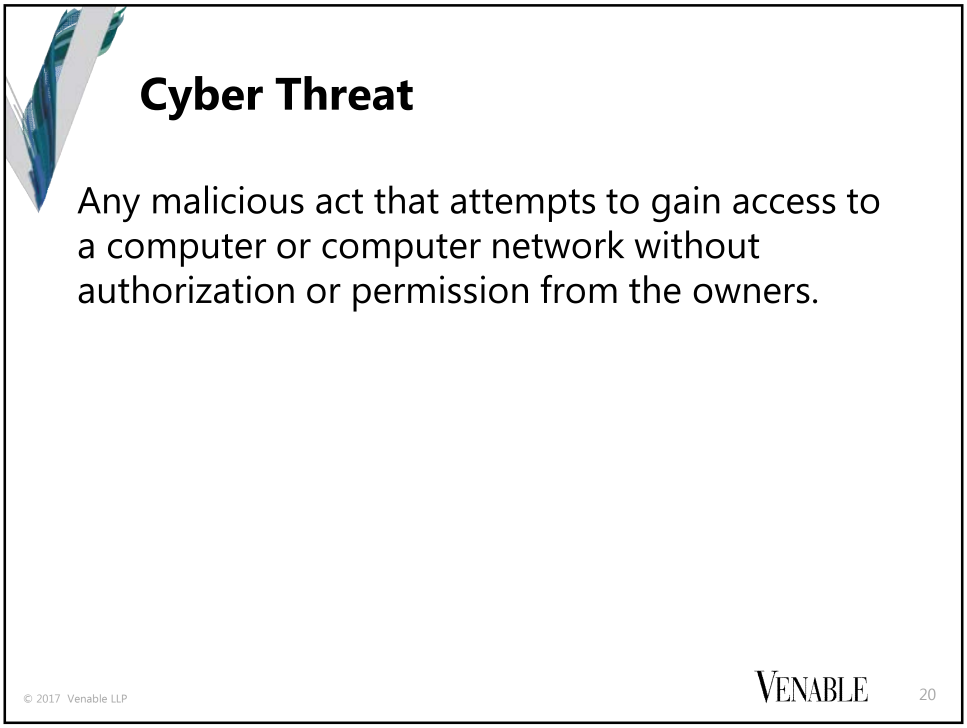


5. Stay Up to Date

- Cybersecurity risk management is not a “one-time” effort
- Legal standards and security threats are constantly evolving
- Consider periodic review and reassessment, particularly following a breach

The Technical Perspective

VENABLE



Cyber Threat

Any malicious act that attempts to gain access to a computer or computer network without authorization or permission from the owners.

VENABLE

$450+ billion/year globally

200% increase in costs
from 2010 to 2015

1 million victims daily

20% increase in attacks per
week from 2012 to 2013

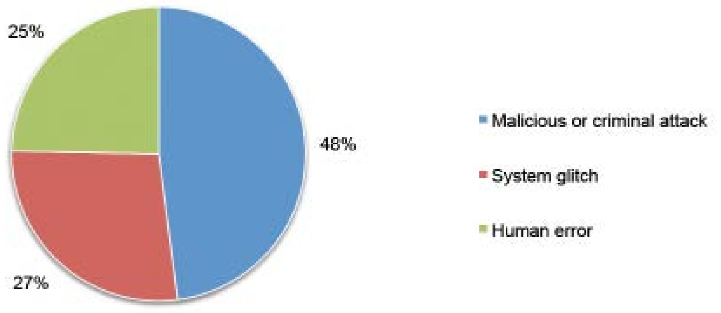
If cybercrime had been a country in 2014,
it would’ve been the 27th largest economy

Source: World Bank, Allianz Cyber Risk Guide

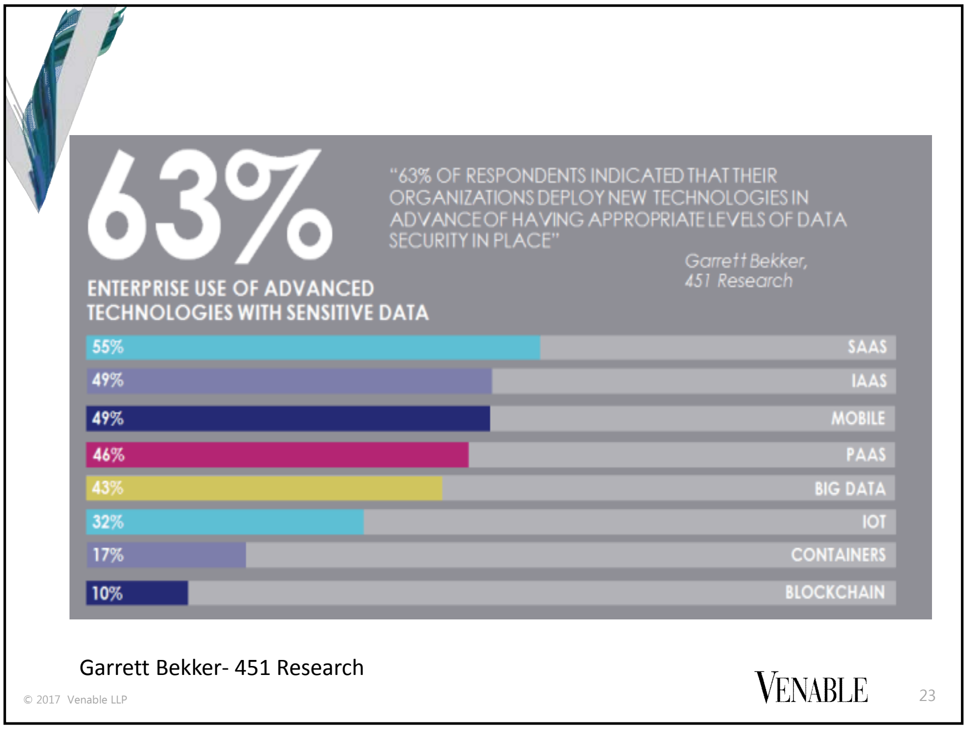
http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Data Breaches

Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach
Consolidated view (n=383)



“2016 Cost of Data Breach Study: Global Analysis,” Ponemon Institute, June 2016



63%

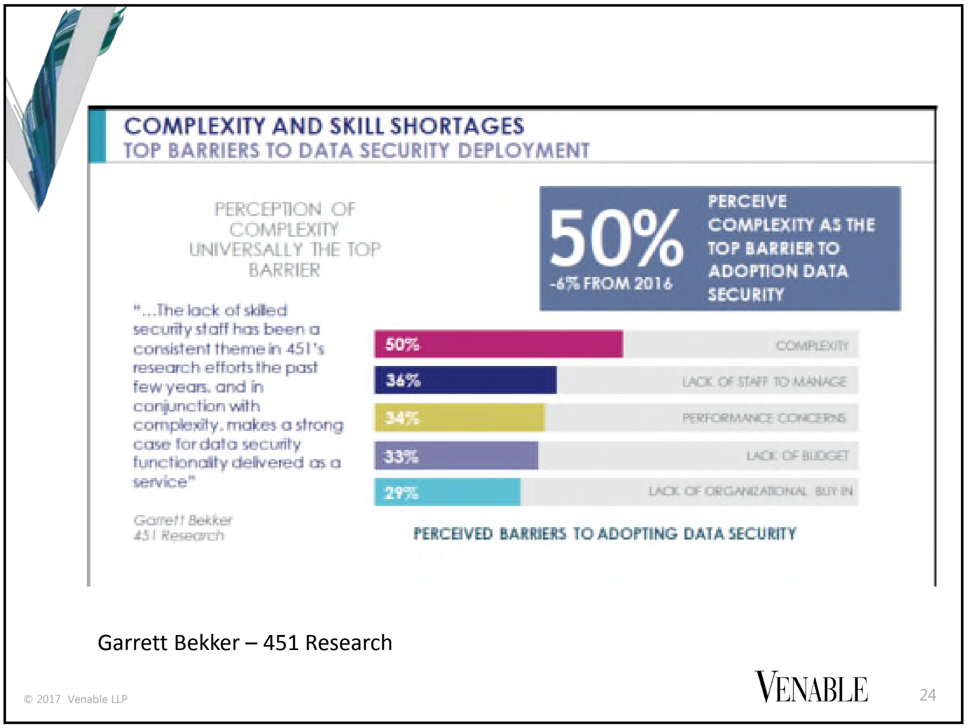
ENTERPRISE USE OF ADVANCED TECHNOLOGIES WITH SENSITIVE DATA

"63% OF RESPONDENTS INDICATED THAT THEIR ORGANIZATIONS DEPLOY NEW TECHNOLOGIES IN ADVANCE OF HAVING APPROPRIATE LEVELS OF DATA SECURITY IN PLACE"

Garrett Bekker, 451 Research

55%	SAAS
49%	IAAS
49%	MOBILE
46%	PAAS
43%	BIG DATA
32%	IOT
17%	CONTAINERS
10%	BLOCKCHAIN

Garrett Bekker- 451 Research



COMPLEXITY AND SKILL SHORTAGES

TOP BARRIERS TO DATA SECURITY DEPLOYMENT

PERCEPTION OF COMPLEXITY UNIVERSALLY THE TOP BARRIER

50% -6% FROM 2016

PERCEIVE COMPLEXITY AS THE TOP BARRIER TO ADOPTION DATA SECURITY

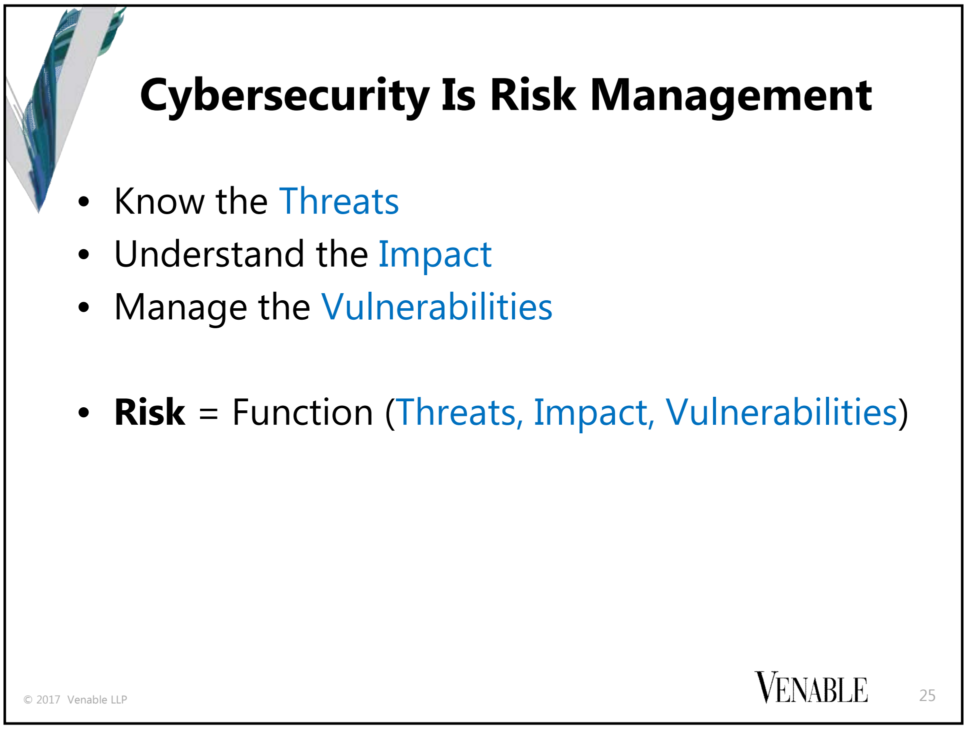
"...The lack of skilled security staff has been a consistent theme in 451's research efforts the past few years, and in conjunction with complexity, makes a strong case for data security functionality delivered as a service"

Garrett Bekker 451 Research

50%	COMPLEXITY
36%	LACK OF STAFF TO MANAGE
34%	PERFORMANCE CONCERNS
33%	LACK OF BUDGET
29%	LACK OF ORGANIZATIONAL BUY IN

PERCEIVED BARRIERS TO ADOPTING DATA SECURITY

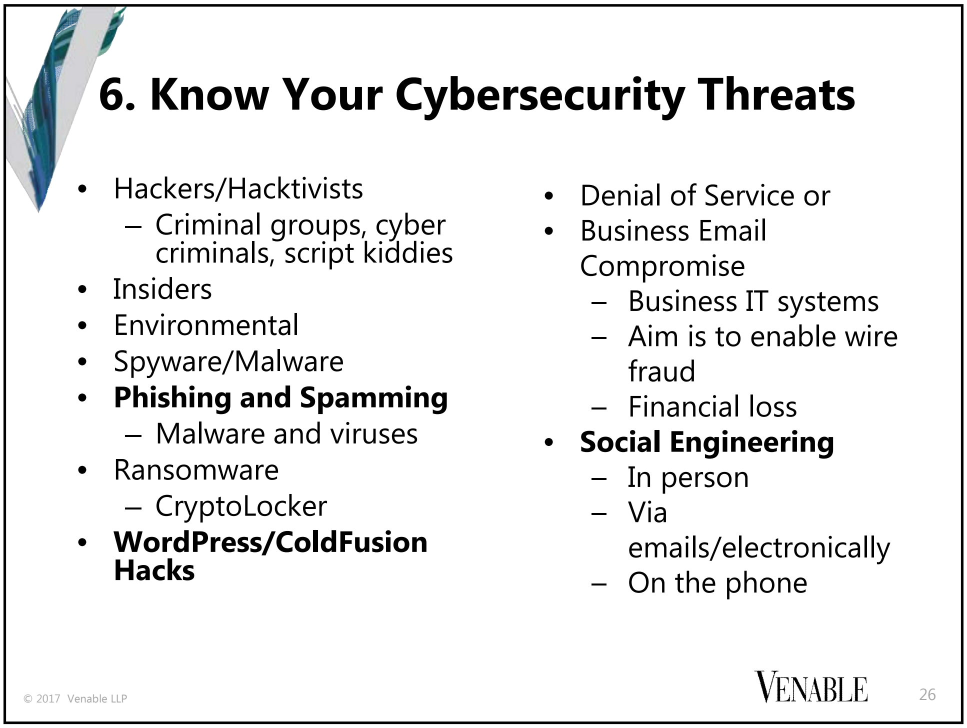
Garrett Bekker – 451 Research



Cybersecurity Is Risk Management

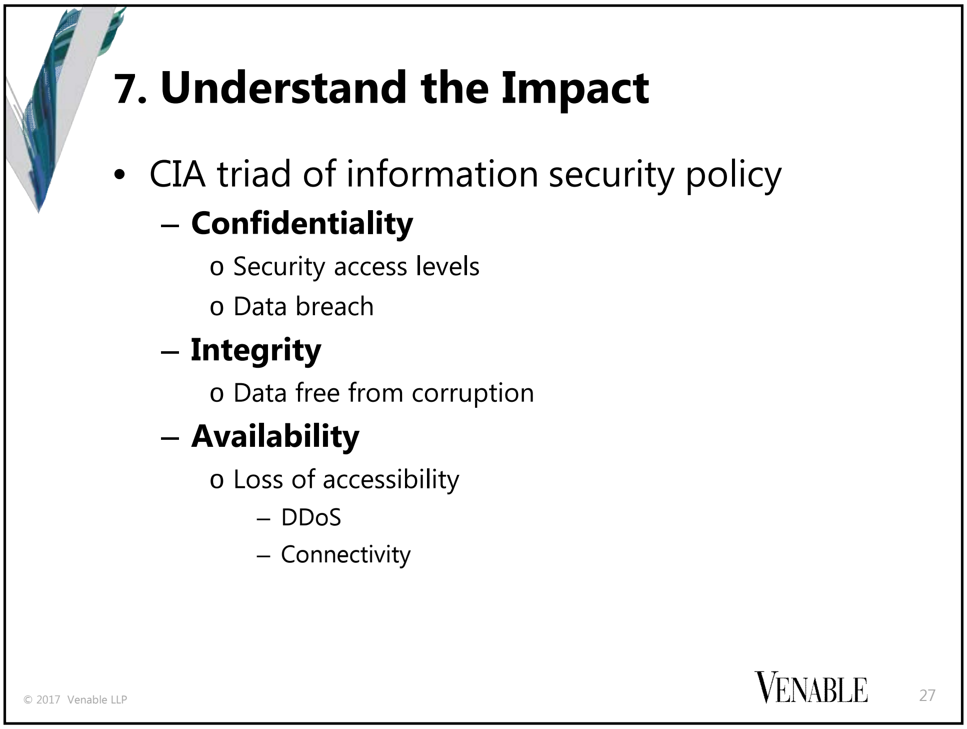
- Know the Threats
- Understand the Impact
- Manage the Vulnerabilities

- **Risk** = Function (Threats, Impact, Vulnerabilities)



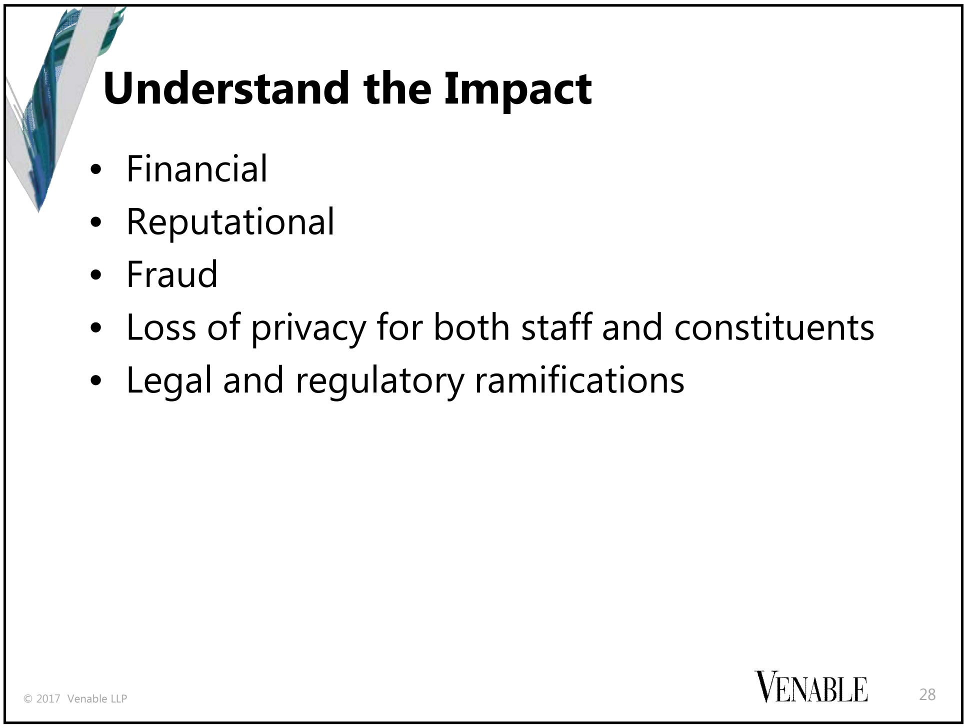
6. Know Your Cybersecurity Threats

- Hackers/Hacktivists
  - Criminal groups, cyber criminals, script kiddies
- Insiders
- Environmental
- Spyware/Malware
- **Phishing and Spamming**
  - Malware and viruses
- Ransomware
  - CryptoLocker
- **WordPress/ColdFusion Hacks**
- Denial of Service or
- Business Email Compromise
  - Business IT systems
  - Aim is to enable wire fraud
  - Financial loss
- **Social Engineering**
  - In person
  - Via emails/electronically
  - On the phone



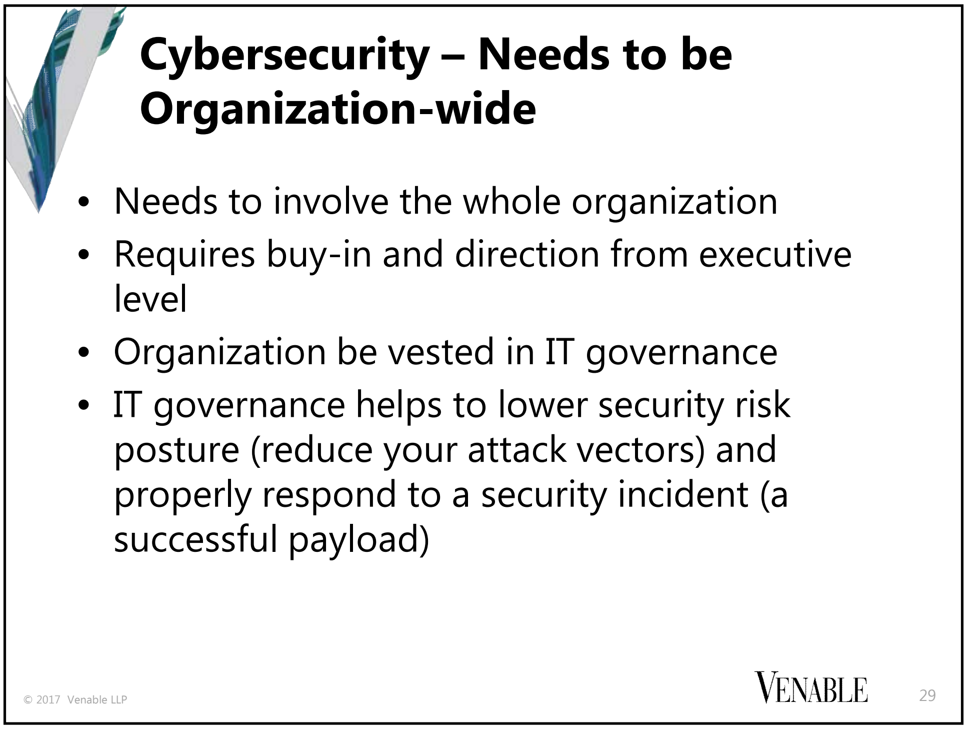
7. Understand the Impact

- CIA triad of information security policy
  - **Confidentiality**
    - Security access levels
    - Data breach
  - **Integrity**
    - Data free from corruption
  - **Availability**
    - Loss of accessibility
      - DDoS
      - Connectivity



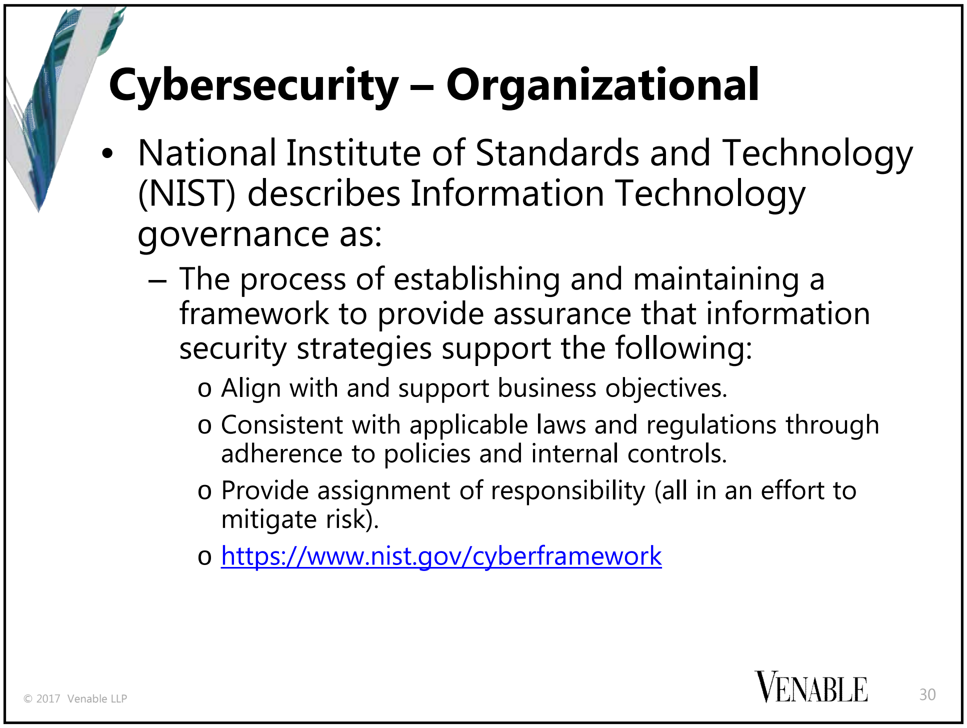
Understand the Impact

- Financial
- Reputational
- Fraud
- Loss of privacy for both staff and constituents
- Legal and regulatory ramifications



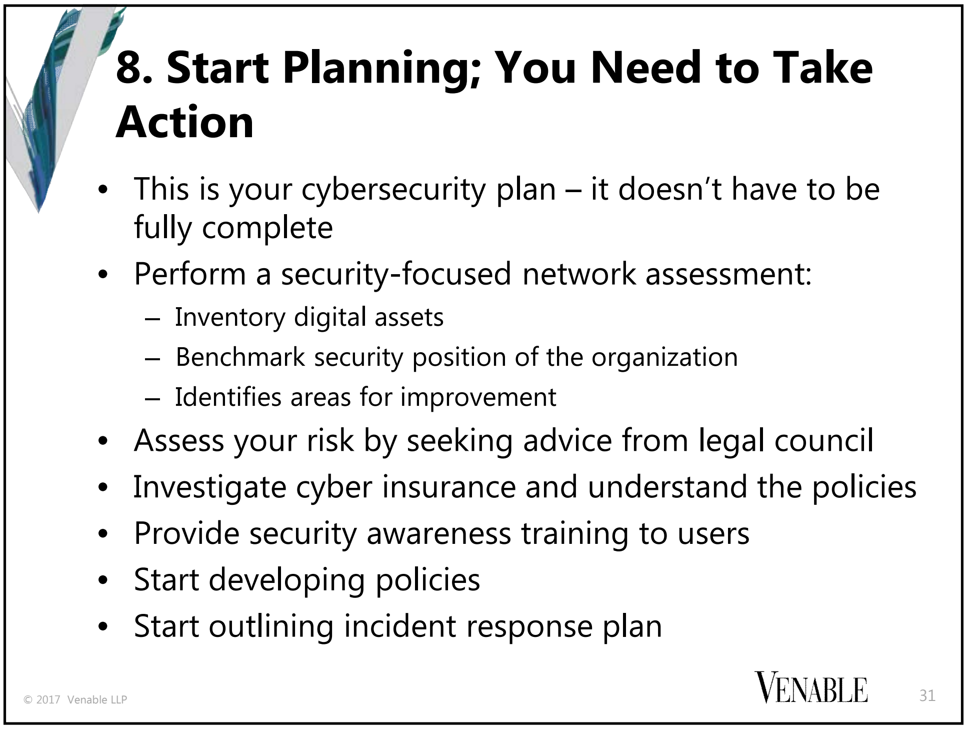
Cybersecurity – Needs to be Organization-wide

- Needs to involve the whole organization
- Requires buy-in and direction from executive level
- Organization be vested in IT governance
- IT governance helps to lower security risk posture (reduce your attack vectors) and properly respond to a security incident (a successful payload)



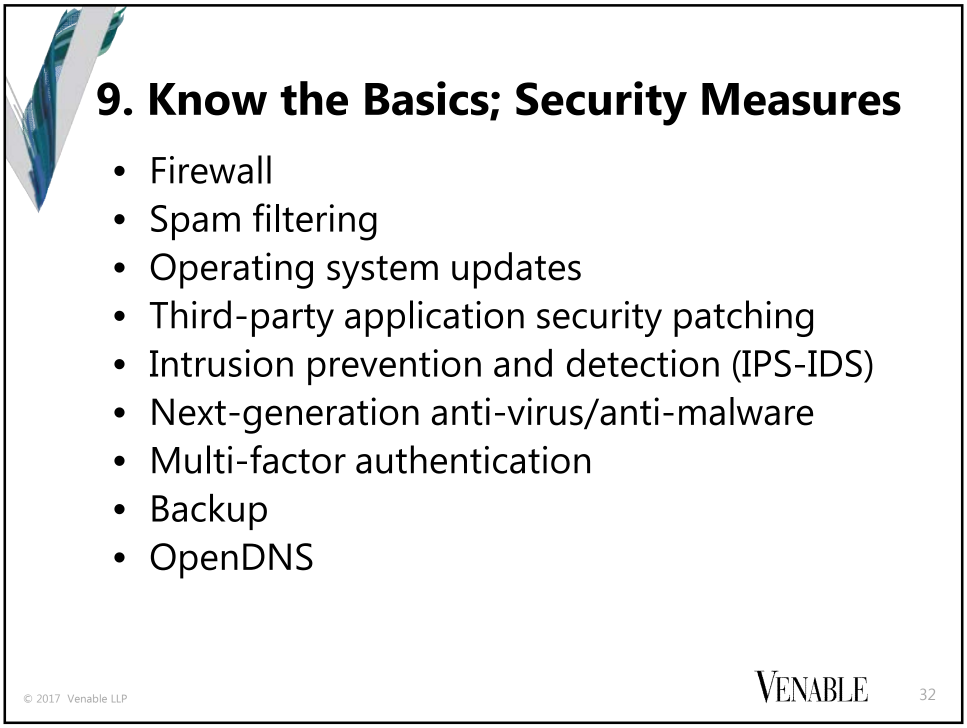
Cybersecurity – Organizational

- National Institute of Standards and Technology (NIST) describes Information Technology governance as:
  - The process of establishing and maintaining a framework to provide assurance that information security strategies support the following:
    - Align with and support business objectives.
    - Consistent with applicable laws and regulations through adherence to policies and internal controls.
    - Provide assignment of responsibility (all in an effort to mitigate risk).
    - https://www.nist.gov/cyberframework



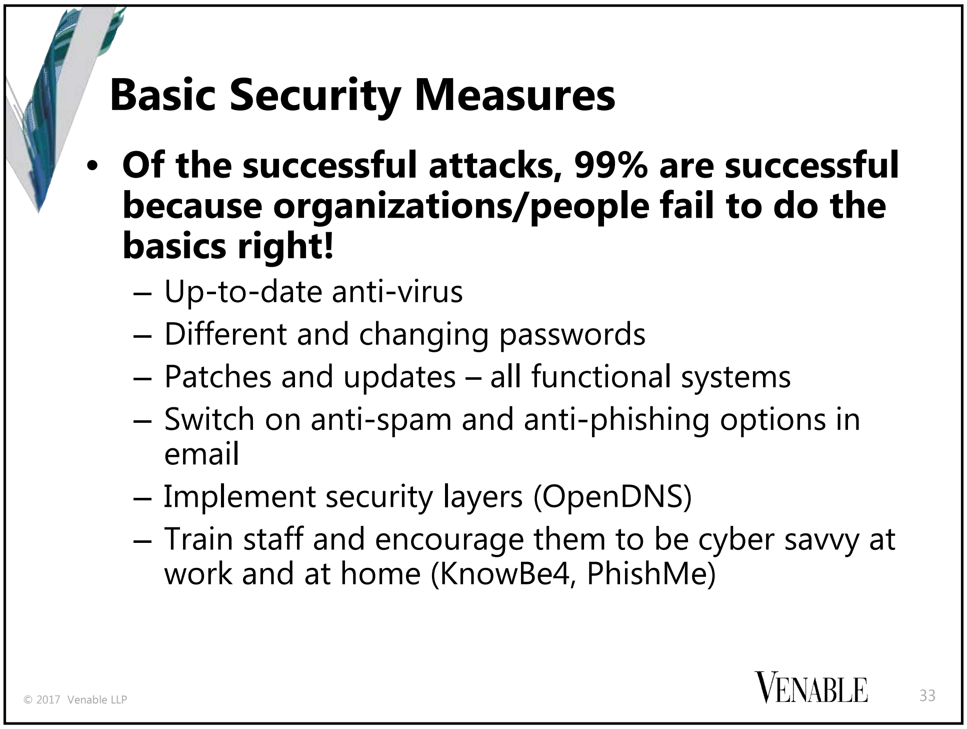
8. Start Planning; You Need to Take Action

- This is your cybersecurity plan – it doesn’t have to be fully complete
- Perform a security-focused network assessment:
  - Inventory digital assets
  - Benchmark security position of the organization
  - Identifies areas for improvement
- Assess your risk by seeking advice from legal council
- Investigate cyber insurance and understand the policies
- Provide security awareness training to users
- Start developing policies
- Start outlining incident response plan



9. Know the Basics; Security Measures

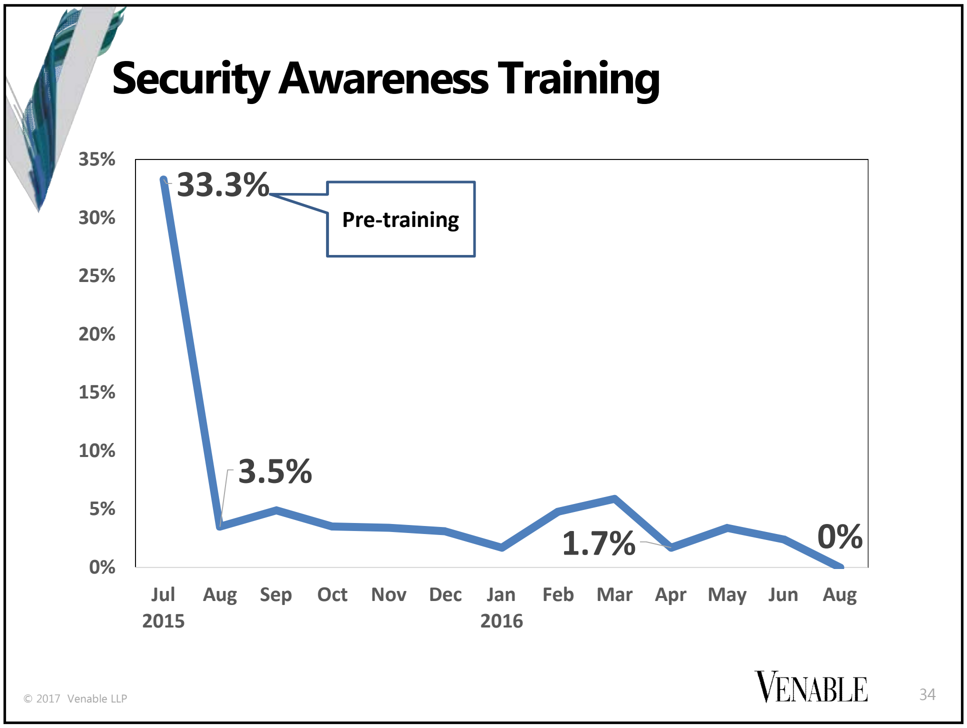
- Firewall
- Spam filtering
- Operating system updates
- Third-party application security patching
- Intrusion prevention and detection (IPS-IDS)
- Next-generation anti-virus/anti-malware
- Multi-factor authentication
- Backup
- OpenDNS



Basic Security Measures

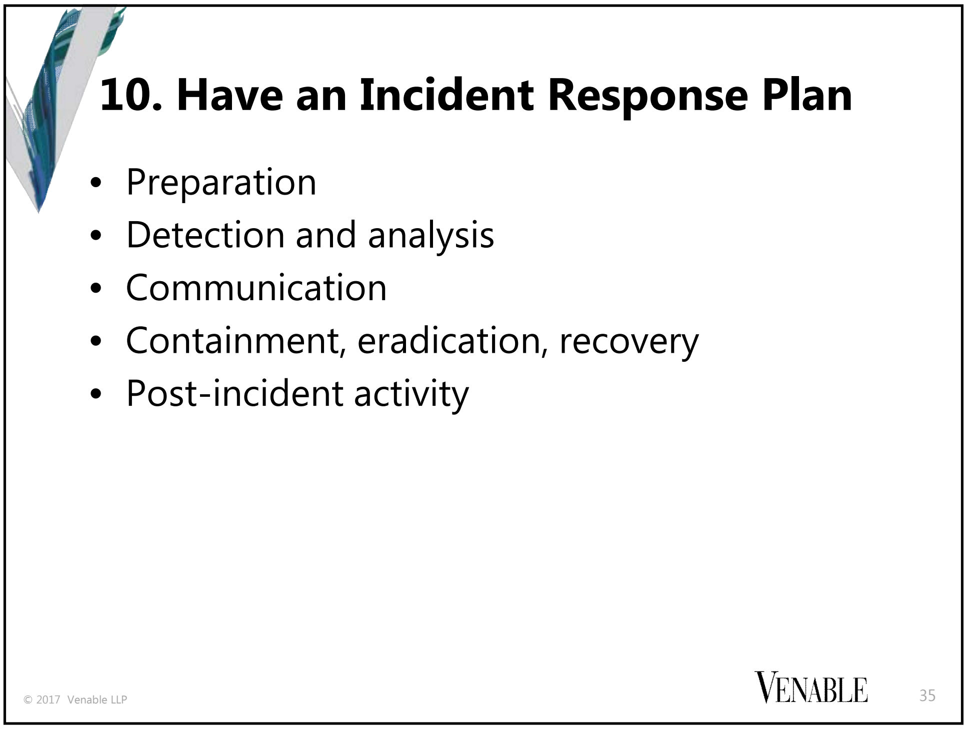
- **Of the successful attacks, 99% are successful because organizations/people fail to do the basics right!**
  - Up-to-date anti-virus
  - Different and changing passwords
  - Patches and updates – all functional systems
  - Switch on anti-spam and anti-phishing options in email
  - Implement security layers (OpenDNS)
  - Train staff and encourage them to be cyber savvy at work and at home (KnowBe4, PhishMe)

VENABLE



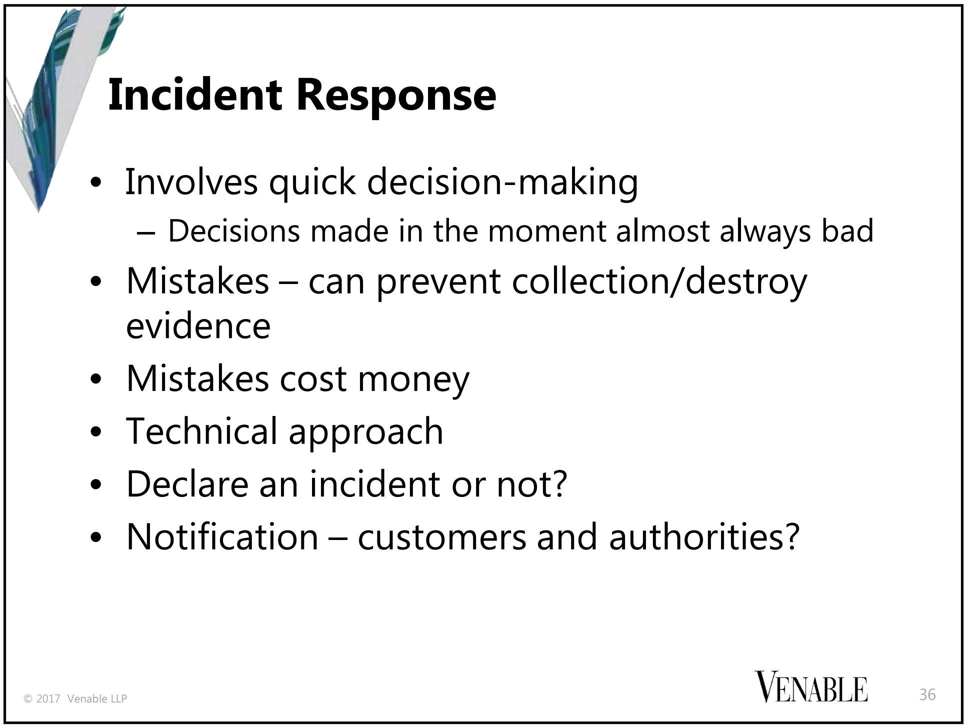
Security Awareness Training

VENABLE



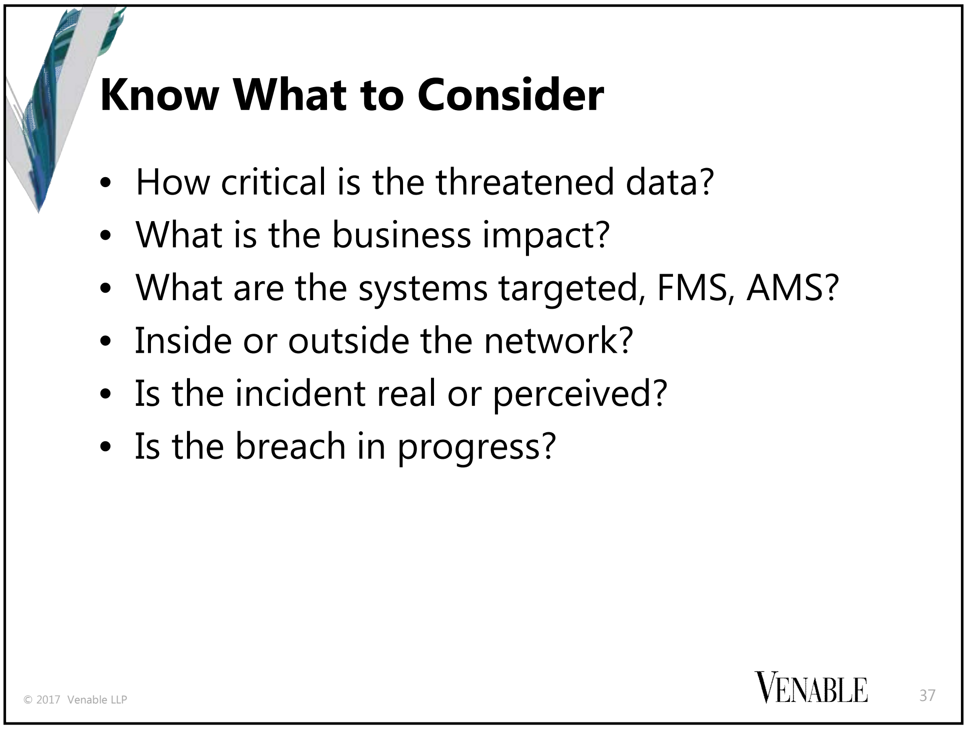
10. Have an Incident Response Plan

- Preparation
- Detection and analysis
- Communication
- Containment, eradication, recovery
- Post-incident activity



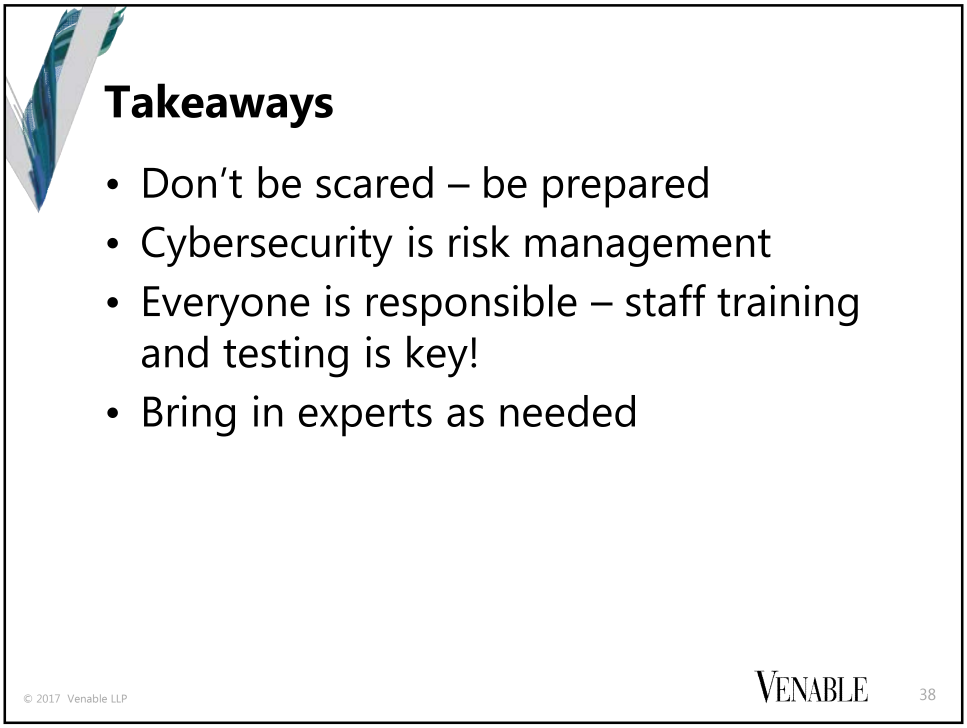
Incident Response

- Involves quick decision-making
  - Decisions made in the moment almost always bad
- Mistakes – can prevent collection/destroy evidence
- Mistakes cost money
- Technical approach
- Declare an incident or not?
- Notification – customers and authorities?



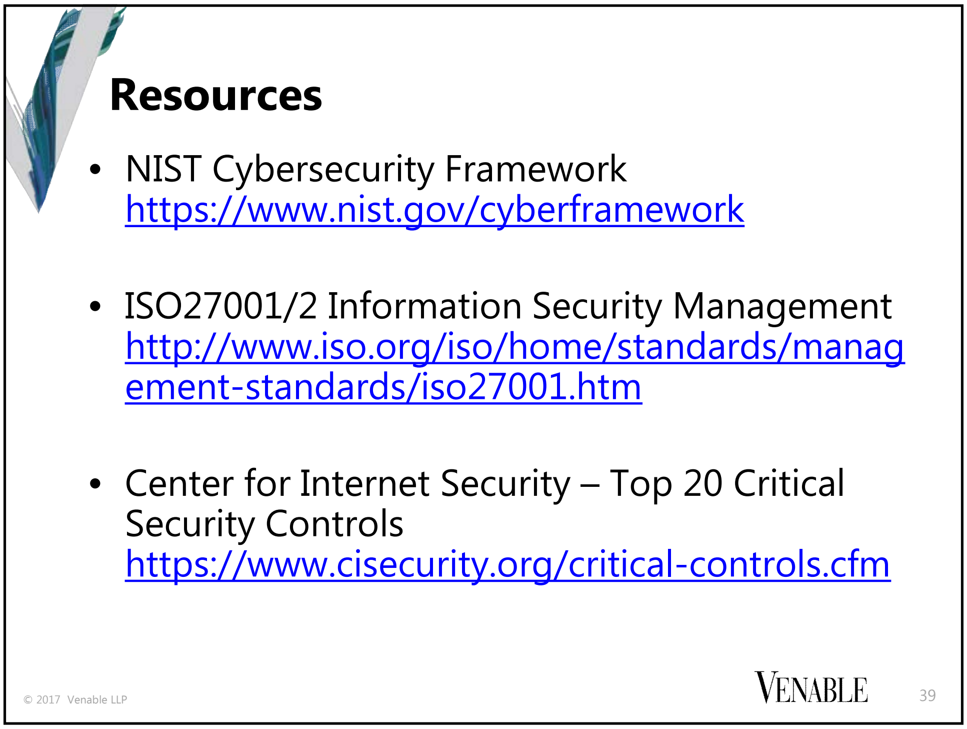
Know What to Consider

- How critical is the threatened data?
- What is the business impact?
- What are the systems targeted, FMS, AMS?
- Inside or outside the network?
- Is the incident real or perceived?
- Is the breach in progress?



Takeaways

- Don’t be scared – be prepared
- Cybersecurity is risk management
- Everyone is responsible – staff training and testing is key!
- Bring in experts as needed

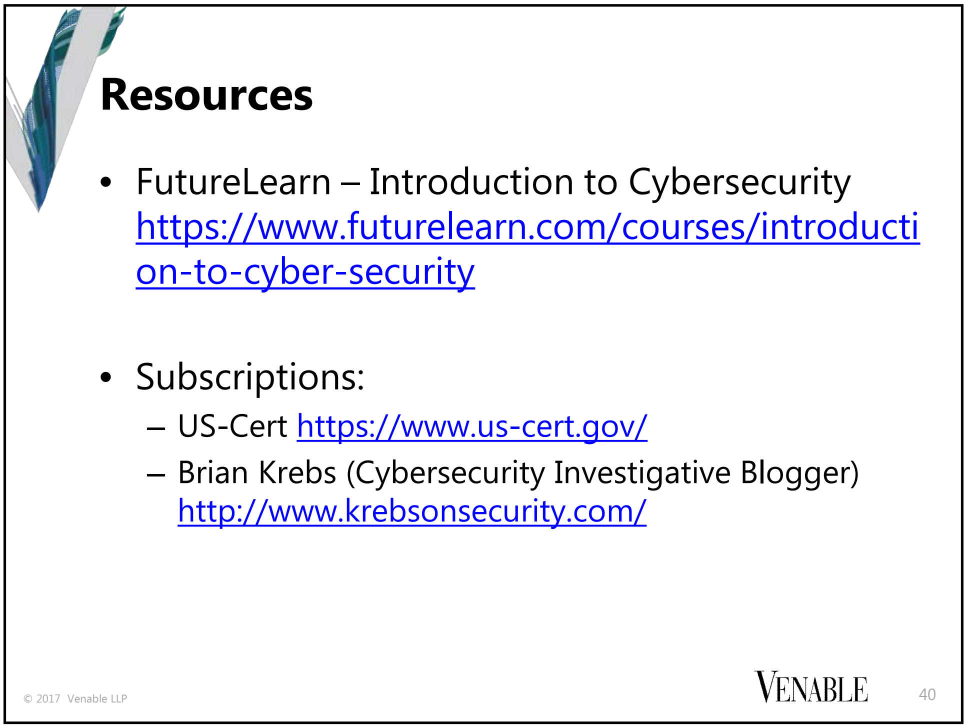


Resources

- NIST Cybersecurity Framework https://www.nist.gov/cyberframework

- ISO27001/2 Information Security Management http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

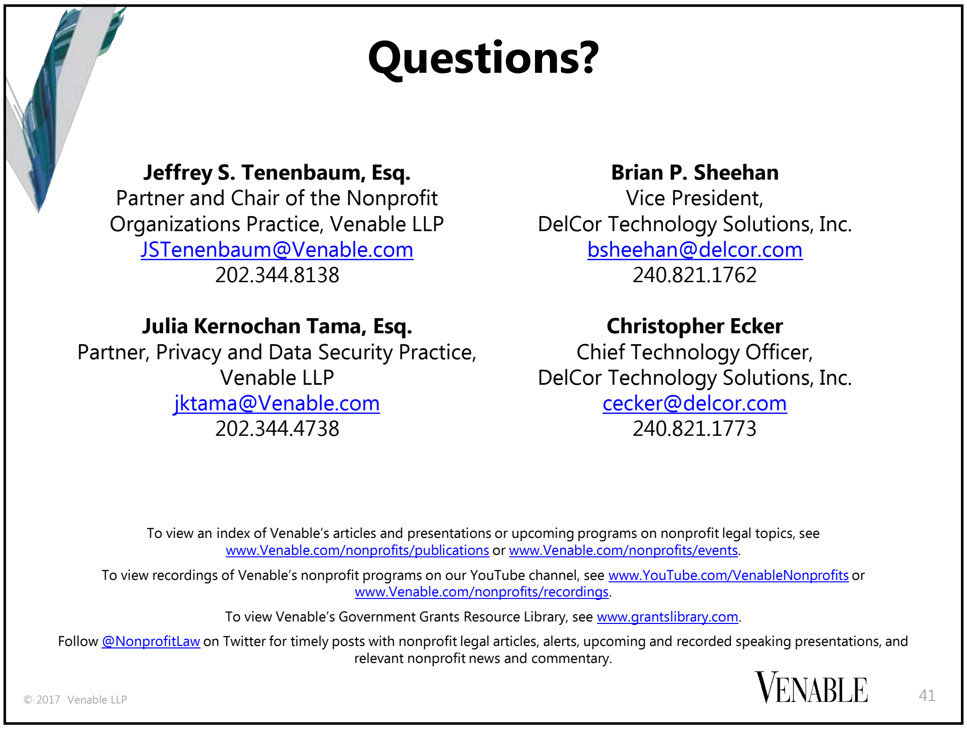
- Center for Internet Security – Top 20 Critical Security Controls https://www.cisecurity.org/critical-controls.cfm



Resources

- FutureLearn – Introduction to Cybersecurity https://www.futurelearn.com/courses/introduction-to-cyber-security

- Subscriptions:
  - US-Cert https://www.us-cert.gov/
  - Brian Krebs (Cybersecurity Investigative Blogger) http://www.krebsonsecurity.com/



Questions?

Jeffrey S. Tenenbaum, Esq.
Partner and Chair of the Nonprofit
Organizations Practice, Venable LLP
JSTenenbaum@Venable.com
202.344.8138

Brian P. Sheehan
Vice President,
DelCor Technology Solutions, Inc.
bsheehan@delcor.com
240.821.1762

Julia Kernochan Tama, Esq.
Partner, Privacy and Data Security Practice,
Venable LLP
jktama@Venable.com
202.344.4738

Christopher Ecker
Chief Technology Officer,
DelCor Technology Solutions, Inc.
cecker@delcor.com
240.821.1773

To view an index of Venable's articles and presentations or upcoming programs on nonprofit legal topics, see www.Venable.com/nonprofits/publications or www.Venable.com/nonprofits/events.

To view recordings of Venable's nonprofit programs on our YouTube channel, see www.YouTube.com/VenableNonprofits or www.Venable.com/nonprofits/recordings.

To view Venable's Government Grants Resource Library, see www.grantslibrary.com.

Follow @NonprofitLaw on Twitter for timely posts with nonprofit legal articles, alerts, upcoming and recorded speaking presentations, and relevant nonprofit news and commentary.

VENABLE

Speaker Biographies

Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

jstenenbaum@Venable.com

Jeffrey Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. He is one of the nation's leading nonprofit attorneys, and also is a highly accomplished author, lecturer, and commentator on nonprofit legal matters. Based in the firm's Washington, DC office, Mr. Tenenbaum counsels his clients on the broad array of legal issues affecting charities, foundations, trade and professional associations, think tanks, advocacy groups, and other nonprofit organizations, and regularly represents clients before Congress, federal and state regulatory agencies, and in connection with governmental investigations, enforcement actions, litigation, and in dealing with the media. He also has served as an expert witness in several court cases on nonprofit legal issues.

Mr. Tenenbaum was the 2006 recipient of the American Bar Association's Outstanding Nonprofit Lawyer of the Year Award, and was an inaugural (2004) recipient of the *Washington Business Journal*'s Top Washington Lawyers Award. He was only a handful of "Leading Lawyers" in the Not-for-Profit category in the prestigious *Legal 500* rankings for the last five years (2012-16). Mr. Tenenbaum was recognized in 2013 as a Top Rated Lawyer in Tax Law by *The American Lawyer* and *Corporate Counsel*. He was the 2015 recipient of the New York Society of Association Executives' Outstanding Associate Member Award, the 2004 recipient of The Center for Association Leadership's Chairman's Award, and the 1997 recipient of the Greater Washington Society of Association Executives' Chairman's Award. Mr. Tenenbaum was listed in the 2012-17 editions of *The Best Lawyers in America* for Non-Profit/Charities Law, and was selected for inclusion in the 2014-16 editions of *Washington DC Super Lawyers* in the Nonprofit Organizations category. In 2011, he was named as one of Washington, DC's "Legal Elite" by *SmartCEO Magazine*. He was a 2008-09 Fellow of the Bar Association of the District of Columbia and is AV Peer-Review Rated by *Martindale-Hubbell*. Mr. Tenenbaum started his career in the nonprofit community by serving as Legal Section manager at the American Society of Association Executives, following several years working on Capitol Hill as a legislative assistant.

ACTIVITIES

Mr. Tenenbaum is an active participant in the nonprofit community who currently serves on the Editorial Board of *The NonProfit Times*, on the Advisory Panel of Wiley/Jossey-Bass' *Nonprofit Business Advisor* newsletter, and on the American Society of Association Executives' Public Policy Committee. He previously served as Chairman and as a member of the ASAE *Association Law & Policy* Editorial Advisory Board and has served on the ASAE Legal Section Council, the ASAE Association Management Company Accreditation Commission, the GWSAE Foundation Board of Trustees, the GWSAE Government and Public Affairs Advisory Council, the Federal City Club Foundation Board of Directors, and the Editorial Advisory Board of Aspen's *Nonprofit Tax & Financial Strategies* newsletter.

AREAS OF PRACTICE

Tax and Wealth Planning

Antitrust

Political Law

Tax Controversies and Litigation

Tax Policy

Tax-Exempt Organizations

Regulatory

INDUSTRIES

Nonprofit Organizations

GOVERNMENT EXPERIENCE

Legislative Aide, United States House of Representatives

BAR ADMISSIONS

District of Columbia

EDUCATION

J.D., Catholic University of America, Columbus School of Law, 1996

B.A., Political Science, University of Pennsylvania, 1990

MEMBERSHIPS

American Society of Association Executives

REPRESENTATIVE CLIENTS

AARP
Academy of Television Arts & Sciences
Air Conditioning Contractors of America
Air Force Association
Airlines for America
American Academy of Physician Assistants
American Alliance of Museums
American Association for Marriage and Family Therapy
American Association for the Advancement of Science
American Bar Association
American Cancer Society
American College of Cardiology
American College of Radiology
American Council of Education
American Institute of Architects
American Nurses Association
American Red Cross
American Society for Microbiology
American Society of Anesthesiologists
American Society of Association Executives
American Thyroid Association
America's Health Insurance Plans
Anti-Defamation League
Association for Healthcare Philanthropy
Association for Talent Development
Association of Clinical Research Professionals
Association of Corporate Counsel
Association of Fundraising Professionals
Association of Global Automakers
Association of Private Sector Colleges and Universities
Auto Care Association
Better Business Bureau Institute for Marketplace Trust
Biotechnology Innovation Organization
Brookings Institution
Carbon War Room
Catholic Relief Services
CFA Institute
The College Board
CompTIA
Council on Foundations
CropLife America
Cruise Lines International Association
Cystic Fibrosis Foundation
Democratic Attorneys General Association
Design-Build Institute of America
Entertainment Industry Foundation
Erin Brockovich Foundation
Ethics Resource Center
Foundation for the Malcolm Baldrige National Quality Award
Gerontological Society of America
Global Impact
Good360
Goodwill Industries International
Graduate Management Admission Council
Habitat for Humanity International
Homeownership Preservation Foundation
Human Rights Campaign
Independent Insurance Agents and Brokers of America
InsideNGO
Institute of Management Accountants
International Association of Fire Chiefs
International Rescue Committee
International Sleep Products Association
Jazz at Lincoln Center

LeadingAge
The Leukemia & Lymphoma Society
Lincoln Center for the Performing Arts
Lions Club International
March of Dimes
ment'or BKB Foundation
National Air Traffic Controllers Association
National Association for the Education of Young Children
National Association of Chain Drug Stores
National Association of College and University Attorneys
National Association of College Auxiliary Services
National Association of County and City Health Officials
National Association of Manufacturers
National Association of Music Merchants
National Athletic Trainers' Association
National Board of Medical Examiners
National Coalition for Cancer Survivorship
National Coffee Association
National Council of Architectural Registration Boards
National Council of La Raza
National Fallen Firefighters Foundation
National Fish and Wildlife Foundation
National Propane Gas Association
National Quality Forum
National Retail Federation
National Student Clearinghouse
The Nature Conservancy
NeighborWorks America
New Venture Fund
NTCA - The Rural Broadband Association
Nuclear Energy Institute
Patient-Centered Outcomes Research Institute
Peterson Institute for International Economics
Professional Liability Underwriting Society
Project Management Institute
Public Health Accreditation Board
Public Relations Society of America
Romance Writers of America
Telecommunications Industry Association
The Tyra Banks TZONE Foundation
U.S. Chamber of Commerce
United States Tennis Association
Volunteers of America
Water Environment Federation
Water For People
WestEd
Whitman-Walker Health

HONORS

Recipient, New York Society of Association Executives' Outstanding Associate Member Award, 2015

Recognized as "Leading Lawyer" in *Legal 500*, Not-For-Profit, 2012-16

Listed in *The Best Lawyers in America* for Non-Profit/Charities Law (Woodward/White, Inc.), 2012-17

Selected for inclusion in *Washington DC Super Lawyers*, Nonprofit Organizations, 2014-16

Served as member of the selection panel for the *CEO Update* Association Leadership Awards, 2014-16

Recognized as a Top Rated Lawyer in Taxation Law in *The American Lawyer* and *Corporate Counsel*, 2013

Washington DC's Legal Elite, *SmartCEO Magazine*, 2011

Fellow, Bar Association of the District of Columbia, 2008-09

Recipient, American Bar Association Outstanding Nonprofit Lawyer of the Year Award, 2006

Recipient, *Washington Business Journal* Top Washington Lawyers Award, 2004

Recipient, The Center for Association Leadership Chairman's Award, 2004

Recipient, Greater Washington Society of Association Executives Chairman's Award, 1997

Legal Section Manager / Government Affairs Issues Analyst, American Society of Association Executives, 1993-95

AV® Peer-Review Rated by *Martindale-Hubbell*

Listed in *Who's Who in American Law* and *Who's Who in America*, 2005-present editions

PUBLICATIONS

Mr. Tenenbaum is the author of the book, *Association Tax Compliance Guide*, now in its second edition, published by the American Society of Association Executives. He also is a contributor to numerous ASAE books, including *Professional Practices in Association Management*, *Association Law Compendium*, *The Power of Partnership*, *Essentials of the Profession Learning System*, *Generating and Managing Nondues Revenue in Associations*, and several Information Background Kits. In addition, he is a contributor to *Exposed: A Legal Field Guide for Nonprofit Executives*, published by the Nonprofit Risk Management Center. Mr. Tenenbaum is a frequent author on nonprofit legal topics, having written or co-written more than 1,000 articles.

SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer on nonprofit legal topics, having delivered over 850 speaking presentations. He served on the faculty of the ASAE Virtual Law School, and is a regular commentator on nonprofit legal issues for *NBC News*, *The New York Times*, *The Wall Street Journal*, *The Washington Post*, *Los Angeles Times*, *The Washington Times*, *The Baltimore Sun*, *ESPN.com*, *Washington Business Journal*, *Legal Times*, *Association Trends*, *CEO Update*, *Forbes Magazine, The Chronicle of Philanthropy, The NonProfit Times, Politico, Bloomberg Business, Bloomberg BNA, EO Tax Journal,* and other periodicals. He also has been interviewed on nonprofit legal topics on Washington, DC CBS-TV affiliate, the Washington, DC Fox-TV affiliate's morning new program, Voice of America Business Radio, Nonprofit Spark Radio, The Inner Loop Radio, and Through the Noise podcasts.

AREAS OF PRACTICE

Privacy and Data Security

Legislative and Government Affairs

Advertising and Marketing

Advertising and Marketing Litigation

Regulatory

Anti-Money Laundering

Payment Processing and Merchant Services

INDUSTRIES

Financial Services

Consumer Financial Services

Cybersecurity Risk Management Services

GOVERNMENT EXPERIENCE

Judiciary Committee Counsel, U.S. Senator Charles E. Schumer (D-NY)

BAR ADMISSIONS

New York

District of Columbia

EDUCATION

J.D., Yale Law School, 2005

Julia Kernochan Tama

Partner

Washington, DC Office

T 202.344.4738 F 202.344.8300

jktama@Venable.com

Julia Kernochan Tama is a partner in the firm's Regulatory Affairs Group. She focuses on helping clients comply with privacy and data security laws in their business operations, and represent their interests before federal and state authorities. Ms. Tama's practice includes:

- Advising clients in a range of industries – including financial services, information services, online and mobile ad tech, and retail – on compliance in the areas of financial privacy, marketing and advertising, consumer protection, e-commerce, children's privacy, health privacy, and other legal and self-regulatory regimes;
- Representing clients facing inquiries or enforcement actions by the Federal Trade Commission, members and committees of Congress, state attorneys general, and other agencies, including under laws prohibiting "unfair or deceptive" business practices;
- Preparing privacy policies and advising on contract provisions related to privacy and data security;
- Performing assessments of privacy practices, including for companies responding to or carrying out due diligence in a potential acquisition;
- Guiding clients through all phases of responding to a data security incident, from the initial forensic investigation through issuing any required notifications and handling inquiries from regulators, customers, and the media; and
- Advocating on behalf of clients concerned about the potential impact of proposed agency regulation or legislation, including by monitoring policy developments and drafting comments on rulemakings.

Ms. Tama regularly advises on an array of laws and regulations including the Gramm-Leach-Bliley Act and California's Financial Information Privacy Act, the Children's Online Privacy Protection Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Telephone Consumer Protection Act and Telemarketing Sales Rule, breach notification obligations, the Digital Advertising Alliance Self-Regulatory Principles, and other industry self-regulatory frameworks.

Prior to joining Venable, Ms. Tama served as Judiciary Committee Counsel to U.S. Senator Charles E. Schumer (D-NY), where her portfolio included privacy, data security, consumer protection, child Internet safety, and foreign intelligence surveillance issues.

PUBLICATIONS

- August 2016, The Download - August 2016, The Download
- July 2016, The Download - July 2016, The Download
- June 2016, The Download - June 2016, The Download

M.P.A., Woodrow Wilson School of Public and International Affairs, Princeton University, 2005

B.A., Swarthmore College, 1998

Phi Beta Kappa

- June 28, 2016, Keep Calm and Carry On: Data Protection Post Brexit, The Download
- May 2016, The Download - May 2016, The Download
- April 2016, The Download - April 2016, The Download
- April 14, 2016, Enforcing your website terms, health app developers get a regulatory check-up, and more in this edition of Advertising Law News & Analysis, Advertising Alert
- April 6, 2016, FTC Creates Compliance Tool for Mobile Health App Developers; Simultaneously Releases Business Guidance, *All About Advertising Law Blog*
- March 2016, The Download - March 2016, The Download
- January 2016, Data Breach Notification Law Handbook v.2.0
- January 2016, The Download - January 2016, The Download
- December 2015, The Download - December 2015, The Download
- November 2015, The Download - November 2015, The Download
- October 2015, The Download - October 2015, The Download
- September 2015, The Download - September 2015, The Download
- July 2015, The Download - July 2015, The Download
- June 2015, The Download - June 2015, The Download
- May 2015, The Download - May 2015, The Download
- April 2015, The Download - April 2015, The Download
- March 2015, The Download - March 2015, The Download
- February 2015, The Download - February 2015, The Download
- December 2014, The Download - December 2014, The Download
- November 2014, The Download - November 2014, The Download
- September, 2014, The Download - September 2014, The Download
- July 2014, Data Breach Notification Law Handbook
- June 2014, The Download - June 2014, The Download
- February 2014, The Download - February 2014, The Download
- November 2013, The Download - November 2013, The Download
- October 2013, The Download - October 2013, The Download
- August 2013, The Download - August 2013, The Download
- August 2013, Digital Advertising Alliance Releases New Mobile Guidance, *Media & Technology E-Bulletin, ABA Antitrust Section*
- June 2013, The Download - June 2013, The Download
- March 2013, The Download - March 2013, The Download
- February 4, 2013, The Download - January 2013, The Download
- January 3, 2013, Advertising News & Analysis - January 3, 2013, Advertising Alert
- December 20, 2012, It's Beginning to Look a Lot Like… COPPA, *All About Advertising Law Blog*
- December 13, 2012, Advertising News & Analysis – December 13, 2012, Advertising Alert
- November 2012, Mobile Data Privacy: Snapshot of an Evolving Landscape, *Journal of Internet Law*
- August 2012, FTC Modifies COPPA Rule Proposal, Advertising Alert
- August 2012, The Download - August 2012, The Download
- June 2012, The Download - June 2012, The Download
- February 2012, The Download - February 2012, The Download
- December 2011, The Download - December 2011, The Download
- October 2011, The Download - October 2011, The Download
- May 2011, Special Report: Summary of FTC Request for Comments on Updating Its "Dot Com Disclosures: Information About Online Advertising", The Download

- May 2011, The Download - May 2011, The Download
- May 10, 2011, Top Five Privacy and Data Security Issues for Nonprofit Organizations
- March 2011, The Download - March 2011, The Download
- January 2011, The Download - January 2011, The Download
- December 2010, Special Issue: Federal Trade Commission Report on Privacy, The Download
- November 2010, The Download - November 2010, The Download
- August 2010, The Download - August 2010, The Download
- April 2010, The Download - April 2010, The Download
- February 2010, The Download - February 2010 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
- November 2009, The Download - November 2009 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
- September 2009, The Download - September 2009 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
- July 2009, Electronic Health Records: "Meaningful Use" in a Land Rush, Healthcare Alert
- July 2009, Self-Regulatory Principles for Online Behavioral Advertising
- May 2009, The Download - May 2009 - Developments in E-Commerce, Privacy, Marketing, and Information Services Law and Policy, The Download
- April 21, 2009, Law Enforcement Risks for Advertisers, Affiliates & Networks; FTC Declares Identity Theft Red Flags Rule Applies to Health Care Professionals; FTC Asserts Jurisdiction to Investigate Security of Personal Health Data; Federal Stimulus Package Includes Dramatic Changes to Health Privacy and Security Law; NCTA v. FCC: The Use of Consumer Information for Marketing Purposes; Massachusetts Revises and Further Delays Implementation of New Data Security Regulations, The Download

SPEAKING ENGAGEMENTS

- May 19, 2015, "Data Breach: From HIPAA to State Laws and Beyond" for IAPP KnowledgeNet
- April 23, 2015, "Payment Security in Card Present Environments" at the Electronic Transaction Association’s Payments Security Day
- April 1, 2015, "The Buck Stops (W)here: C-Suite Responsibilities for Managing Cyber and Data Security Risk" at ETA TRANSACT 15
- March 4, 2015 - March 6, 2015, IAPP Global Privacy Summit 2015
- September 18, 2014 - September 19, 2014, IAPP Privacy Academy and CSA Congress
- September 11, 2014, LIVE Webcast: Children’s Online Privacy Protection Rule: Strengthening Kids' Privacy
- October 22, 2013, Practical and Legal Guidance for Social Media Engagement
- August 7, 2013, "Data Privacy in the Digital Age" at the 24th Annual Direct Response Forum
- July 18, 2013, The Road Map to HIPAA Compliance
- July 17, 2013, The Road Map to HIPAA Compliance
- June 5, 2013, "The State of Mobile in the DAA Program: Key Challenges for Cross-Industry Self-Regulation" at the First Annual DAA Summit
- May 30, 2013, "The Clock Is Ticking: Is COPPA Compliance a 'Mission Impossible'?" for Direct Marketing Association
- September 6, 2012, "Privacy and Information Security Update" for the ABA Section of Antitrust Law
- July 19, 2012, Legal Quick Hit: "Geolocation Data Privacy: Where Are We, and Where Are We Going?" for the Association of Corporate Counsel

- May 3, 2012, Legal Quick Hit: "New Developments in Mobile Privacy" for the Association of Corporate Counsel
- February 1, 2012, "California 'Shine the Light' Law: Could Data Sharing Put You in Class Action Crosshairs?" for the Direct Marketing Association
- May 10, 2011, Legal Quick Hit: "Top Five Privacy and Data Security Issues for Nonprofits" for the Association of Corporate Counsel's Nonprofit Organizations Committee
- March 26, 2011, "Online Advertising and Privacy" at Yale Law School's ISP conference "From Mad Men to Mad Bots: Advertising in the Digital Age"
- June 14, 2010, "Understanding the New Regulations" for International Association of Privacy Professionals Practical Privacy Series, "Privacy in the New Healthcare Era"
- September 23, 2009, The Changing HIPAA Landscape: Seminar on September 23, 2009 in Washington, DC

Brian P. Sheehan

Vice President
DelCor Technology Solutions, Inc.

As DelCor's Vice President, Brian leads the company's infrastructure strategy and support functions for our association and nonprofit clients. Brian is the mastermind behind DelCor's private hosted solution for associations and nonprofits (Cloud Connection)—drawing on 20+ years of working directly with organizations to select, implement, and support network solutions that help them achieve organizational goals.

In recognition of his commitment to extraordinary customer service, Brian was awarded the ASAE All-Star Award for Technology in 2003. An ASAE member, Brian is a frequent speaker at industry events on topics ranging from virtualization to cybersecurity. He currently serves as a volunteer on ASAE's Technology Section Council.

Brian holds a B.S. degree in Business Administration from West Virginia University and an M.S. degree in Information Technology Systems and Telecommunications from Johns Hopkins University.

Chris Ecker

Chief Technology Officer
DelCor Technology Solutions, Inc.

Chris Ecker joined DelCor as a Network Systems Consultant in August 1999 and was promoted to his latest position of Chief Technology Officer in 2004. He has more than 17 years of information technology experience, specializing in Windows, virtualization, networking and security focused technologies.

In his role as CTO, Chris works with the Vice President of Network Systems and Support on areas that include staff development, project planning and service offerings. In addition, he is responsible for developing and communicating standard processes and procedures for technical implementations and on-going network administration. Other areas of focus include testing, developing, and implementing new product and service offerings; performing annual quality assurance reviews for DelCor Partner clients; and staying abreast of emerging technology developments, offerings, and solutions.

Chris holds a B. S. Degree in Accounting from Mount Saint Mary's College. He is a Microsoft Certified Systems Engineer (MCSE) and a VMware Certified Professional and is currently pursuing his Certified Ethical Hacker designation.

Additional Information

VENABLE LLP

cybersecurity risk management

CONTACTS:

Ari M. Schwartz
Managing Director of Cybersecurity Services and Policy
+202.344.4711

John F. Banghart
Senior Director for Technology Risk Management
202.344.4804

Julia Kernochan Tama
Partner, Regulatory
202.344.4738

Jami M. Vibbert
Counsel, Regulatory
202.344.6288

DELIVERING VALUE:

Venable's ability to bring a well-rounded team to an organization allows Venable to understand the needs of the C-suite, information security and/or technology team, and legal department. Our expertise and strong ties to external service providers allow us to provide a synthesized approach that eliminates redundancies, protects privileged information, and reduces cost and risk for our clients.

Helping Your Organization Prioritize and Mitigate Cyber Risk

Venable offers one-of-a-kind cybersecurity risk management services to organizations by bringing together cybersecurity policy drafters and experts, attorneys well-versed in the regulatory and litigation environment, technology experts, and a bi-partisan Legislative and Government Affairs practice. With this well-rounded team, Venable provides a strategic plan on how to focus cybersecurity priorities and where to allocate spend tailored to the organization's risk tolerance, culture, and relevant best practices and governing regulations. In this way, Venable helps organizations incorporate cybersecurity into their existing governance and risk frameworks, ensuring a flexible and resilient approach that reduces the risk of an incident and the risk of reputational harm or liability in the event of an incident.

Venable offers a variety of services designed around the needs of and the risk facing an organization. Some of the services include:

CYBERSECURITY RISK ASSESSMENTS

Cybersecurity risk assessments help an organization understand and identify the risks it faces and prioritizes implementing controls around these risks. These assessments can be organization-wide or targeted at specific systems, departments, or data. They can be one-time assessments or annual updates pursuant to best practice or regulatory requirement. Risk assessments may involve a review of data security, privacy, vendor due diligence, and related processes and procedures; interviews of key stakeholders in the organization; assess training on and implementation of the organization's current cybersecurity and incident response program; compliance with the industry's regulatory framework; and an examination of the technical aspects of the organization's data security procedures and controls.

DETECTION & TECHNOLOGICAL ASSISTANCE & TESTING

Venable has the expertise and relationships to provide or to advise you with respect to various incident detection and prevention technologies, penetration testing, continuous monitoring, information sharing, and others. Venable can provide organizations with an external Chief Information Security Officer.

INCIDENT RESPONSE

Venable reviews, updates, drafts, and tests (via tabletop exercises) incident response plans, as well as provides crisis management in the wake of a potential breach, including assistance with forensic investigations, mitigation measures, reporting and disclosure obligations, law enforcement communications, and regulatory and litigation counsel.

INSURANCE

Venable will counsel organizations as to appropriate coverage amounts and provide recommendations aimed at lowering insurance premiums. Through a review of in-place policies, Venable provides advice on how to qualify for coverage in the event of an incident.

LEGISLATIVE ADVOCACY

Venable provides legislative advocacy on matters of cybersecurity importance, including participation in rulemakings and development of new legal standards.

M&A DUE DILIGENCE

Venable offers detailed cybersecurity risk assessments in the context of M&A due diligence both for a seller before initiation of a sale process to help maximize its sale price, and for a buyer who wants to avoid the potential for reputational harm, liability, and the proprietary nature of intellectual property due to a latent breach or the unreasonable cybersecurity practices of the target.

SERVICES FOR BOARDS OF DIRECTORS & OTHER EXECUTIVES

Venable takes complex technology, process, and management concepts and provides comprehensive, tailored guidance to enable directors and executives to understand the risk they face, their role and accountability in managing it, and how to provide the proper direction and oversight. Venable also drafts, revises, or updates charter documents and mission statements for Board of Directors committees on cybersecurity and governance guidelines to facilitate regular discussion and examination of these issues.

In addition to the above, Venable assists and advises organizations on any issue of data risk management, including:

- Helping its clients address any improvement opportunities following an assessment or to ensure compliance with various regulatory and other cybersecurity requirements.
- Serving in a counseling role on any issue of data risk management, including with respect to cloud services, data analytics, and others.
- Drafting or revising cybersecurity, privacy, information technology, information governance, and related policies and procedures and overseeing large data projects, such as the migration or disposal of data, to confirm legal and cybersecurity best practices are being used.
- Creating vendor due diligence programs.
- Advising organizations on appropriately addressing cybersecurity in SEC disclosures.
- Conducting training of employees on cybersecurity initiatives and programs.
- Creating enforcement programs.

This informational piece is published by the law firm Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations that Venable has accepted an engagement as counsel to address. Attorney Advertising.

VENABLE LLP

CYBERSECURITY ALERT

January 18, 2017

NIST RELEASES UPDATE TO CYBERSECURITY FRAMEWORK

AUTHORS

John Banghart
Ari Schwartz

RELATED INDUSTRIES

Cybersecurity Risk Management Services

ARCHIVES

2017 2013 2009
2016 2012 2008
2015 2011 2007
2014 2010

On January 10, the National Institute of Standards and Technology (NIST) released the long-awaited draft of the Cybersecurity Framework (CSF), draft version 1.1.

Since its initial release, the CSF has gained remarkable recognition in both the public and private sectors as a shared foundation for cybersecurity risk management. The CSF is comprised of three component parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core is comprised of five Functions: Identify, Protect, Detect, Respond, and Recover. Each function is further divided into Categories, Subcategories, and Informative References. The Framework Implementation Tiers and Framework Profiles are tools that help organizations tailor their application of the Framework Core to their particular business model or sector.

The revisions in CSF draft version 1.1 focus on four key areas:

- **Framework Tiers**

  CSF draft version 1.1 clarifies the relationship between the Framework Implementation Tiers and the Framework Profiles. Specifically, CSF draft version 1.1 highlights how an organization can use Framework Tiers during implementation of the Framework. The Framework Tiers put an organization's cybersecurity practices in context within the greater cyber-ecosystem. This context helps organizations to improve their approach to cybersecurity risk management by allowing them to assess their position relative to other stakeholders.

- **Supply Chain Risk Management (SCRM)**

  In recent years, sensitivity to the security of organizational supply chains has become an area of increasing concern across most industry sectors, as the risk introduced through technical and process dependencies becomes better understood.

  To help improve the security of organizational supply chains, NIST has taken several steps in the CSF: adding a SCRM Category to the Framework Core; making several revisions and additions at the sub-category level across multiple categories; and adding SCRM as a criteria in the Implementation Tiers

- **Access Control Category**

  CSF draft version 1.1 modifies the Access Control Category, which falls within the Protect Function. The modified Access Control Category now encompasses authentication, authorization, and identity proofing. Accordingly, the Access Control Category was renamed "Identity Management and Access Control" (PR.AC) in CSF draft version 1.1. The Category was renamed to provide a more accurate characterization of the scope of the Category and Subcategories. To further support the refined Access Control Category, CSF draft version 1.1 includes an additional Subcategory that specifically addresses identity proofing.

- **Measurement**

  NIST is taking the first steps at providing guidance on how to develop metrics and measurement for organizations using the Framework. CSF draft version 1.1 includes a section titled "Measuring and Demonstrating Cybersecurity," which explains the relationship between business objectives and cybersecurity risk management metrics and measures. The updated framework draft also provides a summary of metrics and measures as they relate to the CSF.

The period for submitting comments and feedback to NIST on CSF draft version 1.1 will conclude on

April 10, 2017. Following the comment period, NIST will convene a workshop for interested stakeholders to discuss CSF draft version 1.1. NIST stated that it plans to publish the final CSF version 1.1 around the fall of 2017.

Framework for Improving Critical Infrastructure Cybersecurity

Draft Version 1.1

National Institute of Standards and Technology

January 10, 2017

Note to Reviewers on the Update and Next Steps

The draft Version 1.1 of Cybersecurity Framework refines, clarifies, and enhances the predecessor version 1.0

Version 1.1 can be implemented by first time and current Framework users. Current users can implement Version 1.1 with minimal or no disruption, as refinements were made with the objective of being compatible with Version 1.0.

As with Version 1.0, use of the Version 1.1 is voluntary. Users of Version 1.1 are invited to customize the Framework to maximize organizational value.

The impetus to change and the proposed changes were collected from:

- Feedback and frequently asked questions to NIST since release of Framework Version 1.0 in February 2014,
- 105 responses to the December 2015 request for information (RFI), *Views on the Framework for Improving Critical Infrastructure Cybersecurity*, and
- Comments provided by approximately 800 attendees at a workshop held in Gaithersburg, Maryland on April 6-7, 2016.

In addition, NIST previously released Version 1.0 of the Cybersecurity Framework with a companion document, *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*. This Roadmap highlighted key "areas of improvement" for further "development, alignment, and collaboration." Through both private and public sector efforts, some areas of improvement have advanced enough to be included in the Framework Version 1.1.

Key refinements, clarifications, and enhancements in Framework Version 1.1 include:

Update	Description of Update
A new section on cybersecurity measurement	Added Section 4.0 Measuring and Demonstrating Cybersecurity to discuss correlation of business results to cybersecurity risk management metrics and measures.
Greatly expanded explanation of using Framework for Cyber Supply Chain Risk Management purposes	Considerations of Cyber Supply Chain Risk Management (SCRM) have been added throughout the document. An expanded Section 3.3 Communicating Cybersecurity Requirements with Stakeholders help users better understand Cyber SCRM. Cyber SCRM has also been added as a property of Implementation Tiers. Finally, a Supply Chain Risk Management Category has been added to the Framework Core.
Refinements to better account for authentication, authorization, and identity proofing	The language of the Access Control Category has been refined to account for authentication, authorization, and identity proofing. A Subcategory has been added to that Category. Finally, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.
Better explanation of the relationship between Implementation Tiers and Profiles	Added language to Section 3.2 Establishing or Improving a Cybersecurity Program on using Framework Tiers in Framework implementation. Added language to Framework Tiers to reflect integration of Framework considerations within organizational risk management programs. Updated Figure 2.0 to include actions from the Framework Tiers.

A more detailed review of Version 1.1 refinements, clarifications, and enhancements can be found in Appendix D.

NIST is seeking public comment on this draft Framework Version 1.1, specifically regarding the following questions:

- Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?
- How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?
- For those using Version 1.0, would the proposed changes impact your current use of the Framework? If so, how?
- For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?
- Does this proposed update adequately reflect advances made in the Roadmap areas?
- Is there a better label than "version 1.1" for this update?
- Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?

Feedback and comments should be directed to cyberframework@nist.gov. After reviewing public comments regarding the draft Version 1.1 and convening a workshop on the Framework, NIST intends to publish a final Framework Version 1.1 around the fall of 2017.

Table of Contents

List of Figures

List of Tables

Executive Summary

The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.

To better address these risks, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which established that "[i]t is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The Executive Order also requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. While processes and existing needs will differ, the Framework can assist organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program.

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognized standards for cybersecurity, the Framework can also be used by organizations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.

The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances – and how they implement the practices in the Framework will vary. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks.

The Framework is a living document and will continue to be updated and improved as industry provides feedback on implementation. NIST will continue coordinating industry as directed in the Cybersecurity Enhancement Act of 2014[1]. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions.

Use, evolution, and sharing of best practices of this voluntary Framework are the next steps to improve the cybersecurity of our Nation's critical infrastructure – providing guidance for individual organizations, while increasing the cybersecurity posture of the Nation's critical infrastructure as a whole.

[1] *See* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) became public law 113-274 on December 18, 2014 and may be found at: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.