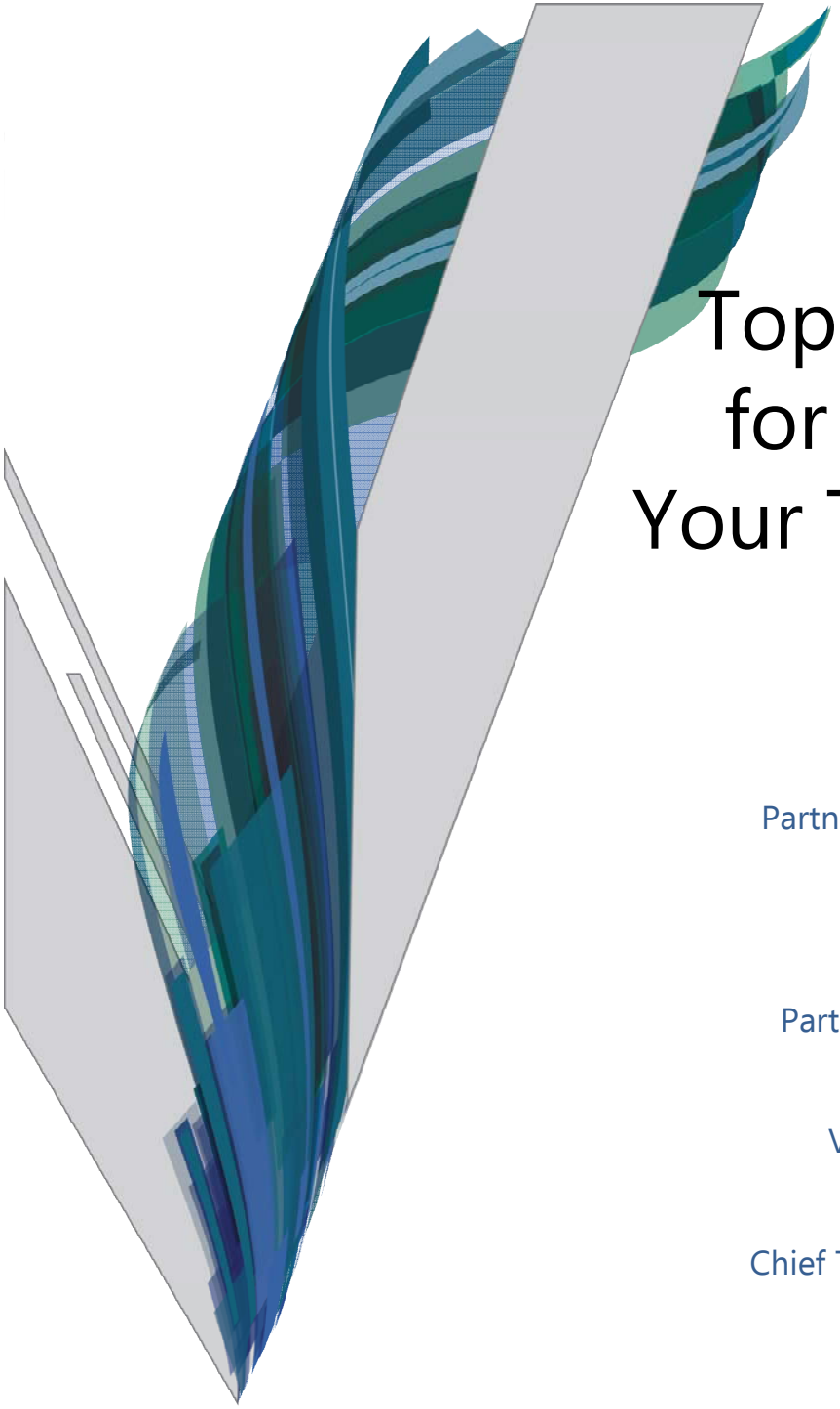


VENABLE

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.

VENABLE

Upcoming Venable Nonprofit Events

Register Now

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

VENABLE

Cybersecurity and Data Security

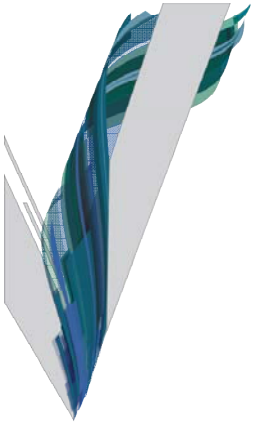
- Cybersecurity and data security are related concepts

- 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

VENABLE

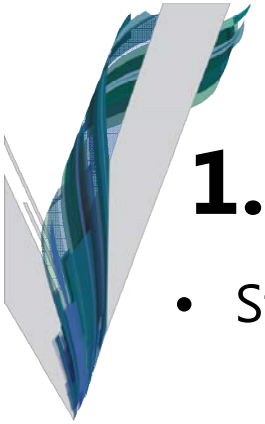


The Legal Perspective

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.

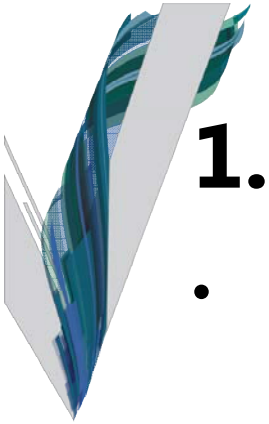


1. Know the Legal Rules

- 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
    - Fines imposed on banks can be passed on to organizations
  - States have enacted statutory requirements similar to PCI DSS

VENABLE

2. Assess Your Risks

Legal Risk → **Legal Assessment** → **Legal Risk Management**

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

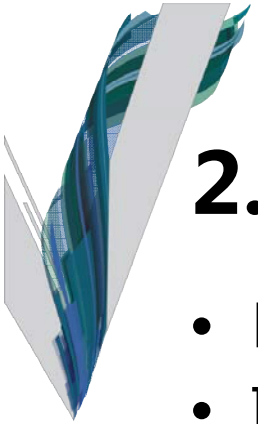
- Policies/Procedures
- Governance
- Incident Response Plan
- Vendor Selection and Contracts
- Training
- Data Mapping

- Reporting and Decision Making
- Legal and Regulatory Compliance Framework

VENABLE

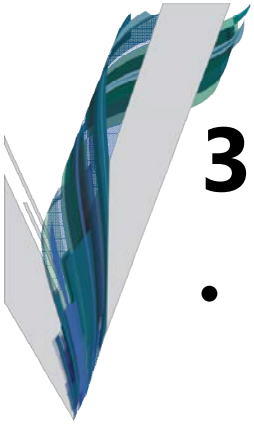
2. Assess Your Risks

- 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

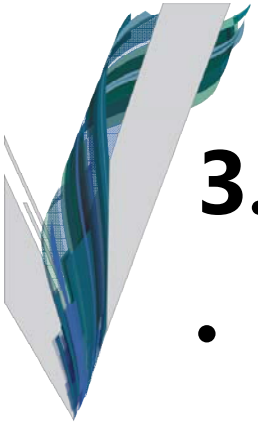
- Perform an enterprise-wide vulnerability assessment
- Implement a comprehensive information security program that addresses any identified vulnerabilities:
  - Periodically review and update the information security program
- Implement appropriate data security policies:
  - Data Classification Policy
  - 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

VENABLE



3. Know Your Vendors

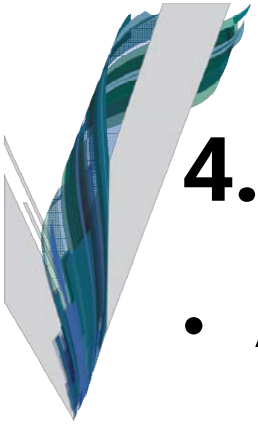
- Specific concerns for vendors hired to help with security assessment and services
- Security findings can be sensitive, and may create liability risks for the organization
- Consider structuring the engagement to ensure products are protected by attorney-client privilege to the extent possible

4. Prepare for the Worst

Cost of a Data Breach:

- Many factors contribute to total costs:
  - Breach response efforts
    - Delivering notices, credit monitoring, legal costs, etc.
  - Reputational costs
    - 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/

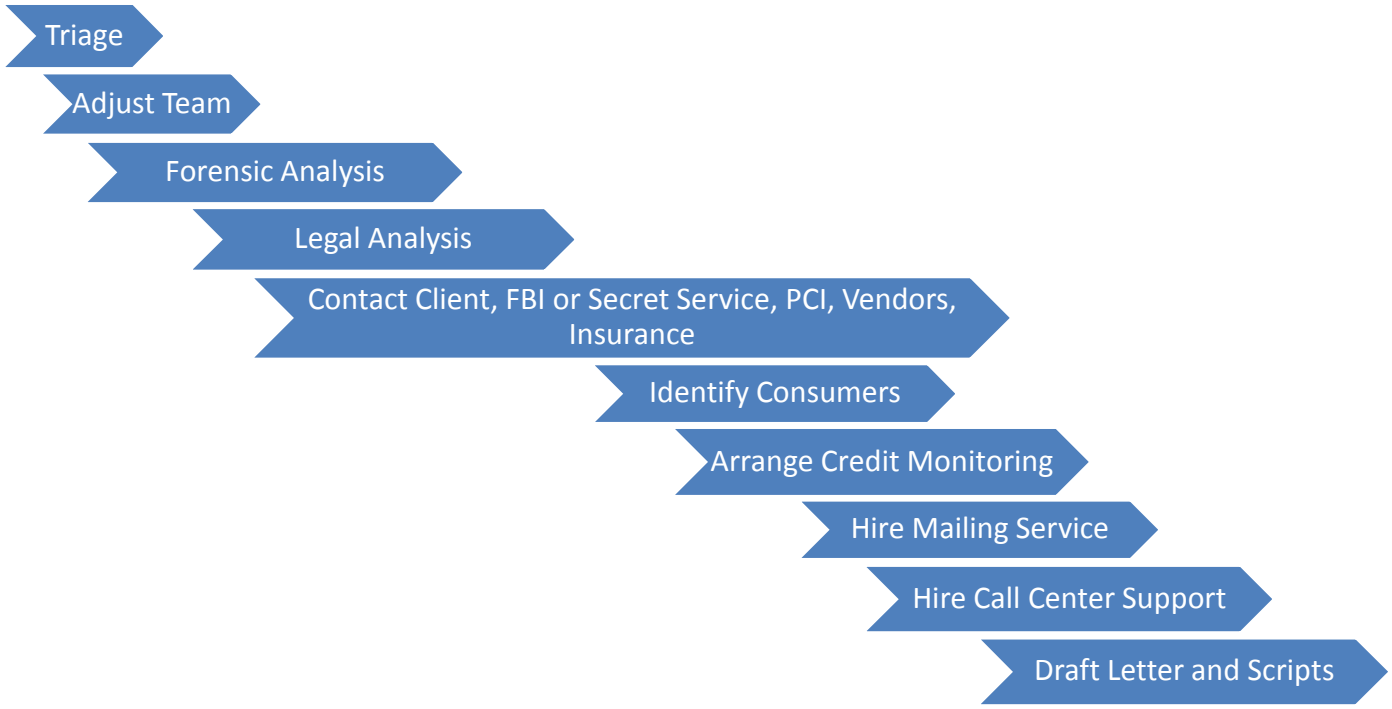


4. Prepare for the Worst

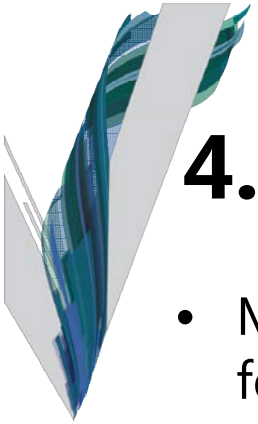
- An effective incident response plan will facilitate:
  - Prompt detection, investigation, recovery (more on this later);
  - Notification of and cooperation with law enforcement officials, if deemed necessary;
  - Notification to external parties affected by the incident, if any, such as customers, 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"

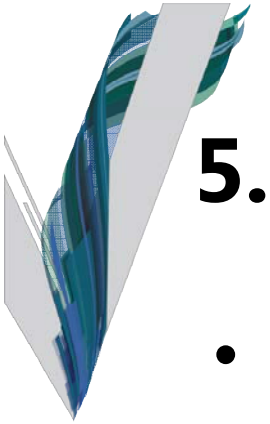


VENABLE



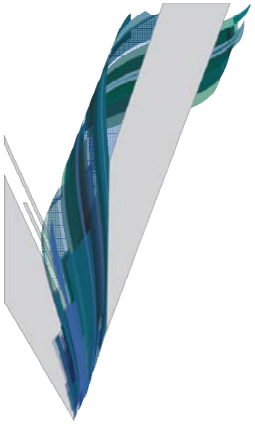
4. Prepare for the Worst

- 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

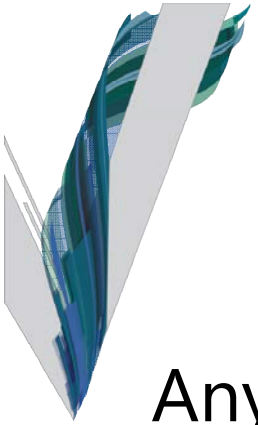


5. Stay Up to Date

- 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



Cyber Threat

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

$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

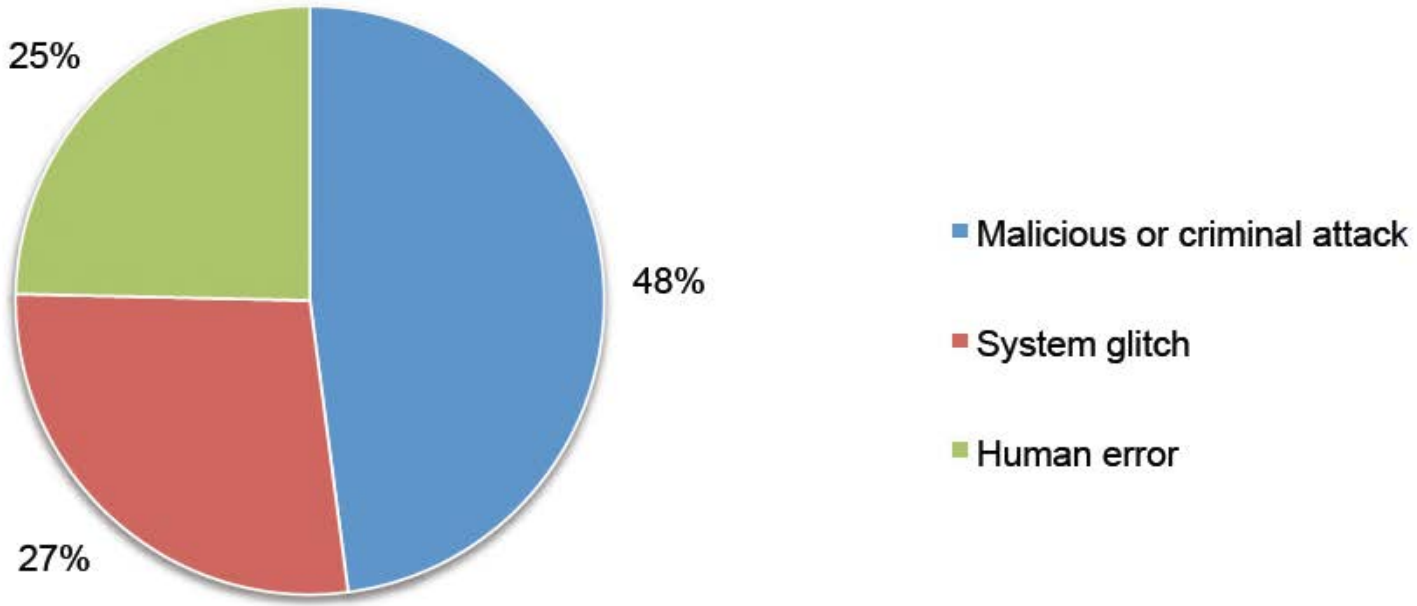
Source: World Bank, Allianz Cyber Risk Guide

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

VENABLE

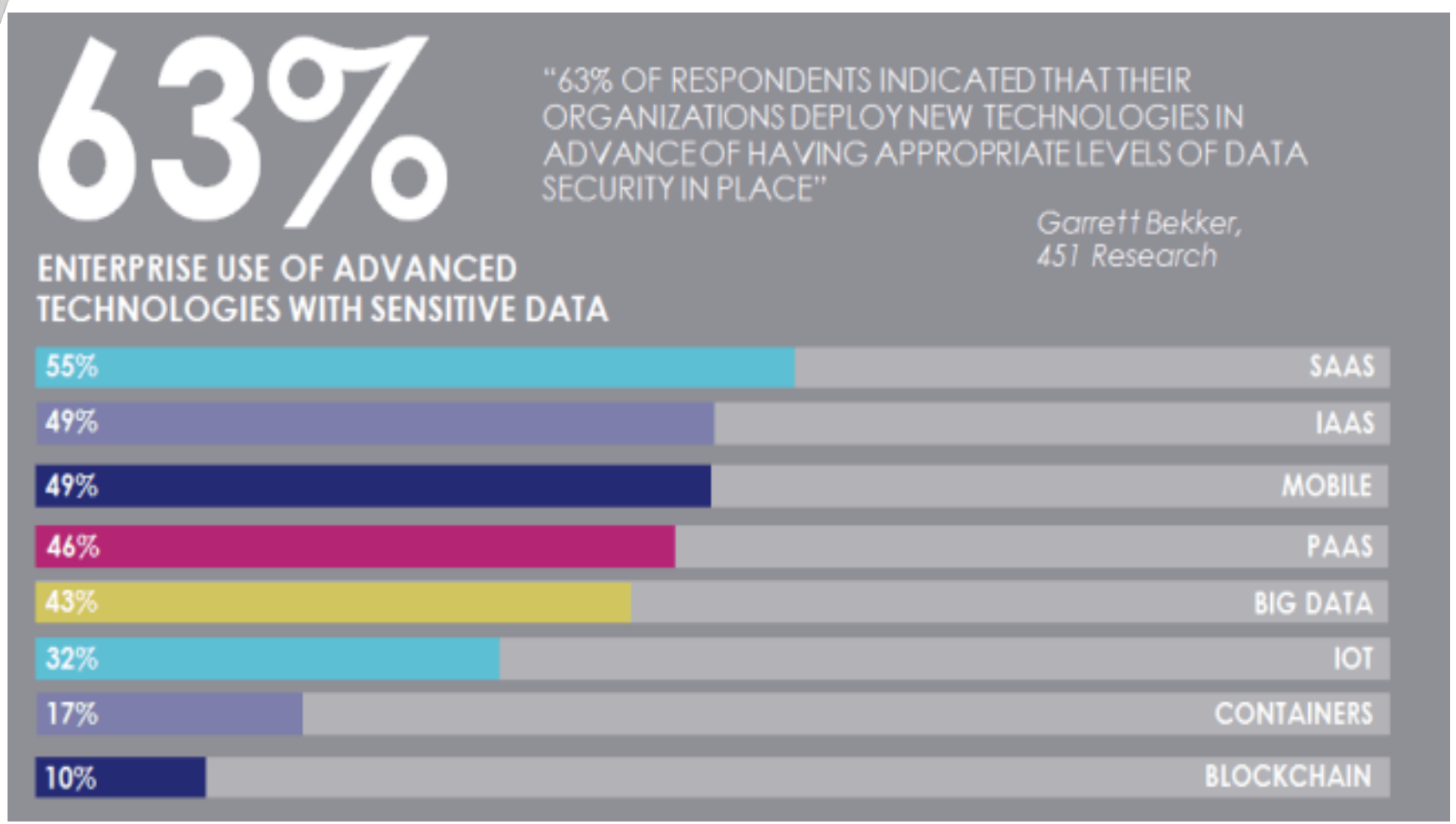
Data Breaches

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

VENABLE



Garrett Bekker- 451 Research

VENABLE

COMPLEXITY AND SKILL SHORTAGES
TOP BARRIERS TO DATA SECURITY DEPLOYMENT

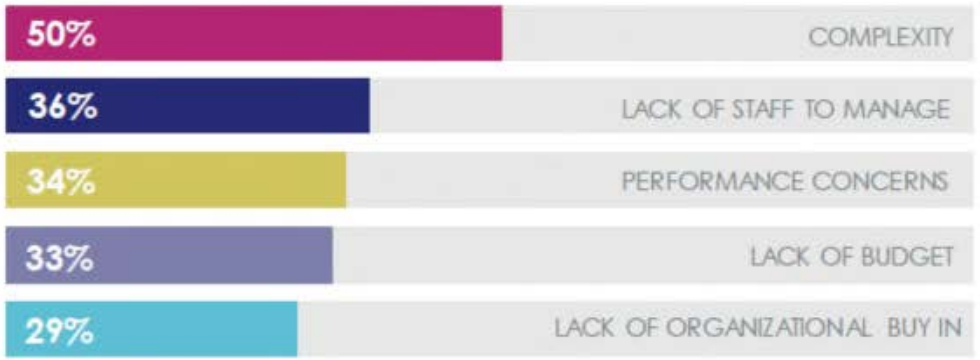
PERCEPTION OF COMPLEXITY UNIVERSALLY THE TOP BARRIER

"...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% -6% FROM 2016

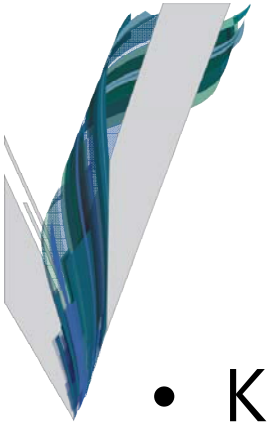
PERCEIVE COMPLEXITY AS THE TOP BARRIER TO ADOPTION DATA SECURITY



PERCEIVED BARRIERS TO ADOPTING DATA SECURITY

Garrett Bekker – 451 Research

VENABLE



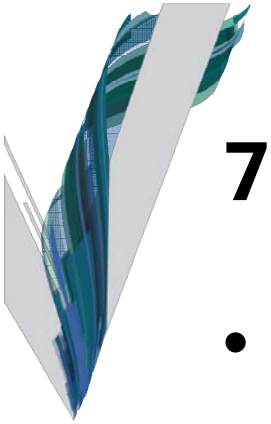
Cybersecurity Is Risk Management

- 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



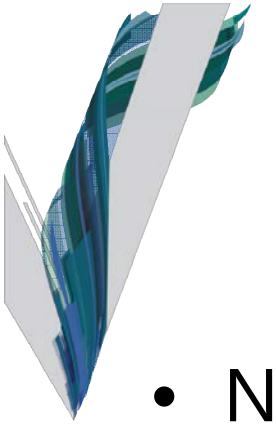
7. Understand the Impact

- 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

VENABLE

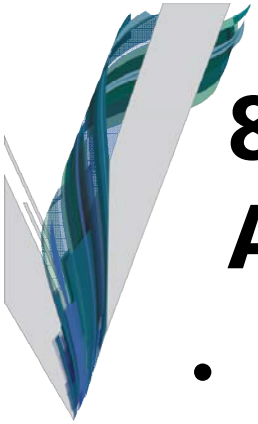


Cybersecurity – Needs to be Organization-wide

- 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

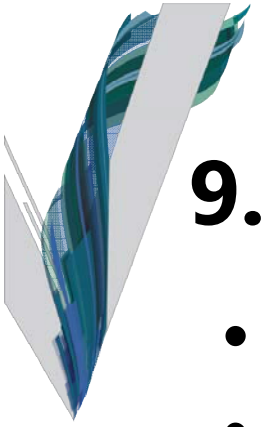
- National Institute of Standards and Technology (NIST) describes Information Technology governance as:
  - The process of establishing and maintaining a framework to provide assurance that information security strategies support the following:
    - Align with and support business objectives.
    - 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

VENABLE



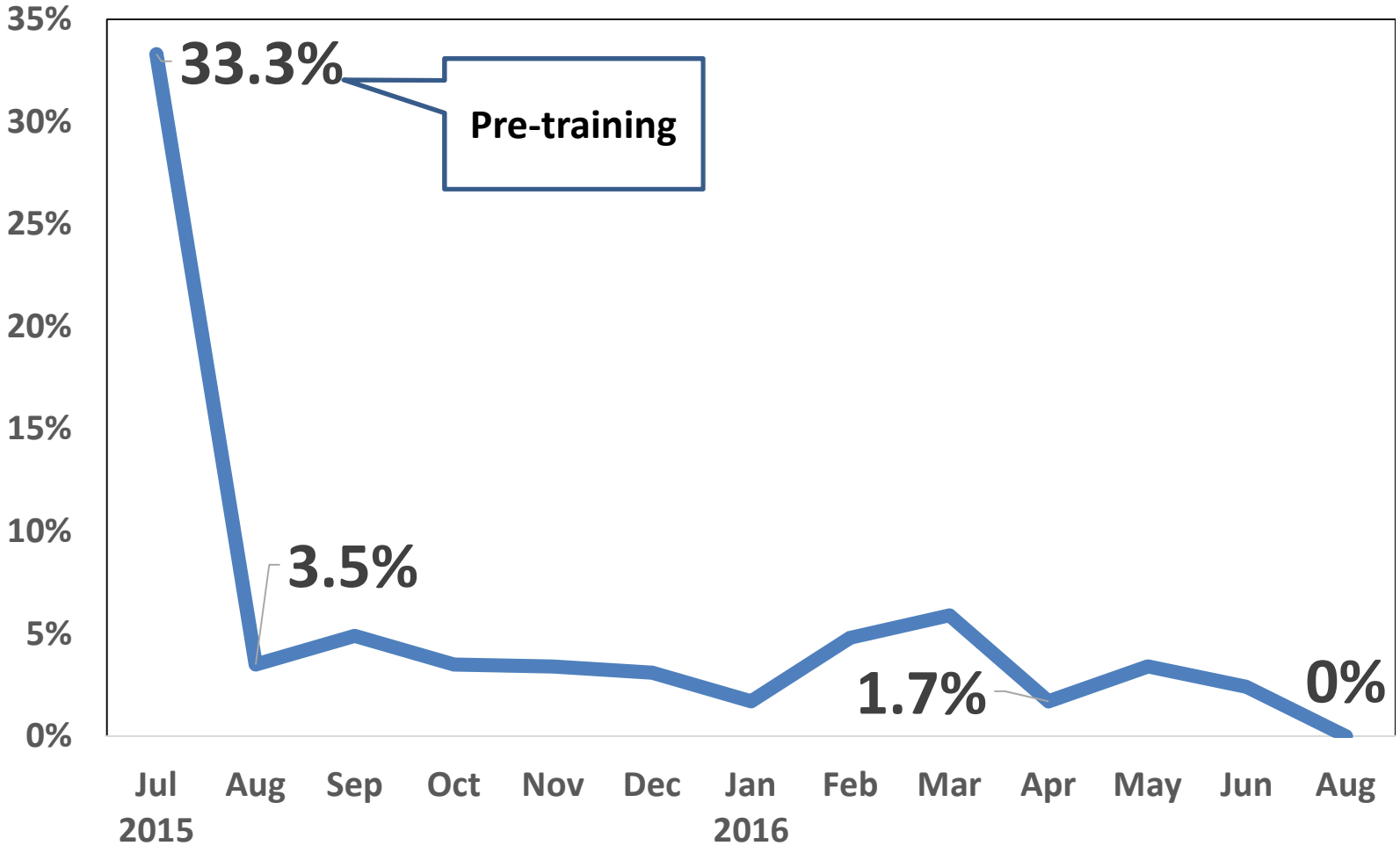
9. Know the Basics; Security Measures

- 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

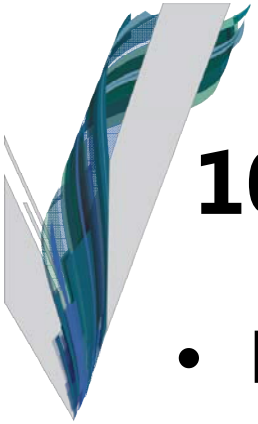
Basic Security Measures

- **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)

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

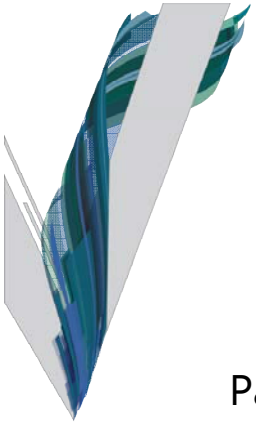
- ISO27001/2 Information Security Management
  http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

- 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