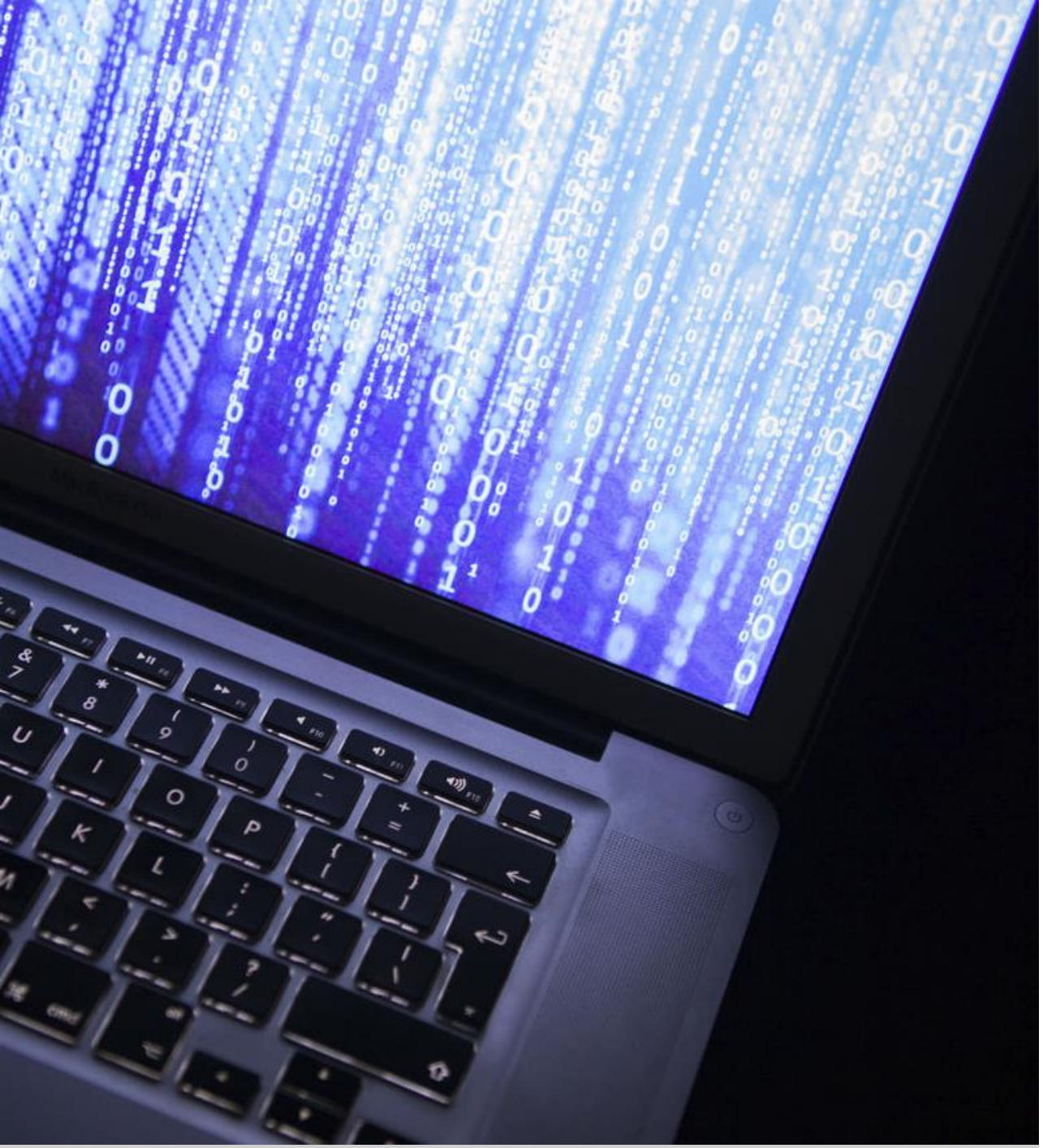


Data Breach Trends and Tips: What State and Local Government Lawyers Need to Know

Practical Law Webinar

January 12, 2017

Presenters:

Mel Gates, Senior Legal Editor, Privacy & Data Security, Practical Law

Zach Ratzman, Director of Public Sector, Practical Law

AGENDA

Why State and Local Governments Should Care

Legal Considerations – A Growing Body of Law

Threats and Attack Trends

The Role of Counsel in Preventing Data Breaches

Why State and Local Governments Should Care

Not a Question of If, But When

- **“Willie Sutton”**
  - State and local governments are data rich government operations
- **Size Does Not Matter**
  - Ease of modern hacking means everyone is a target
- **Accidents Happen**
  - Even if you aren’t hacked, data can still be lost
- **Trusted Insiders**
  - Multiple agendas drive data leakage
- **Lawsuits Happen**
  - No general public immunity under privacy laws

Special Considerations for State and Local Governments

- **State and local government limitations**
  - People: fewer employees to leverage
  - Funding: having to do more with less
  - IT: old(er) systems and equipment
  - Cybersecurity expertise: high demand, difficult to recruit and retain

- **Additional kinds of liability**
  - Legal, financial, ***and political***

- **(Lack of) leadership continuity**
  - Short term costs, long term need

Legal Considerations – A Growing Body of Law

Laws Protect Personal Information

Individual's first name (or initial) + last name, plus* the following:

- **User IDs, passwords, mother's maiden name, answers to security questions**

- **Government identification numbers**
  - SSN, passport, driver's license

- **Financial information**
  - Account numbers

- **Medical or health insurance information**

- **Biometric data**
  - Fingerprints, iris scan, DNA, facial geometry

- **Employee identification number**

*Increasing trend to not require name under certain circumstances

Federal Law

- **Apply to specific data owners and types**

- **Healthcare Information**
  - HIPAA: Health Insurance Portability and Accountability Act
  - HITECH: Health Information Technology for Economic and Clinical Health Act

- **Students' and Children's Personal Information**
  - FERPA: Family Educational Rights and Privacy Act
  - PPRA: Protection of Pupil Rights Amendment
  - COPPA: Children's Online Privacy Protection Act

- **Driver's Privacy Protection Act**

State Law

- **General or state agency data breach statute(s)**
  - Require breach notifications
  - May require incident response plans
- **State data security laws**
  - Can impose proactive data security requirements, such as:
    - Written Information Security Programs (WISPs)
    - Risk assessments
    - Safeguards
    - Service provider governance
  - Increasing number of states call for **reasonable security measures**
- **Sector-specific laws**
  - Student data protection
  - Medical privacy
  - Others

Contracts and Industry Standards

- **Many organizations are obligated to protect data under contracts related to:**
  - Business partner and interagency agreements
  - Payment processing, including through the:
    - Payment Card Industry (PCI) Data Security Standard (DSS)
    - NACHA, the Electronic Payments Association®, operating rules for ACH transactions (such as direct payments from bank accounts)

- **Increasingly relevant to state and local governments as their use of online transactions increases**

Standard of Care?

- **Adopting widely accepted standards and practices mitigates risk**
- **Industry standards and best practices support privacy and information security programs**
  - Fair Information Practice Principles (FIPPs)
  - The NIST Cybersecurity Framework
  - Sector-specific best practices support particular needs

Cybersecurity Information Sharing

- **Helps organizations learn from others**
- **Creates a safer community through increased threat awareness**
- **Supported by federal law and public-private partnerships**
  - Cybersecurity Act of 2015
  - Federal guidance, including privacy protections
  - Information sharing and analysis organizations (ISAOs, ISACs)
    - Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (issued Feb. 13, 2015) fosters standardization

Threats and Attack Trends

Understanding the Threats: *Insiders*

- **Employee negligence**
  - Security failures
  - Lost (and poorly secured) mobile devices
- **Employee ignorance**
  - Improper storage and disposal of information
  - Lack of education and awareness
  - Duped by phishing and other scams
  - Well-intentioned “working around” controls
- **Malicious or politically motivated employees**
  - Intentional misconduct

Examples of Insider Threats

- **Minnesota County Settles Breach Class Action for $1 million**
  - In July 2016, a federal judge preliminarily approved a $1 million settlement between a Minnesota county and a class of county residents whose personal information had been accessed by a county employee without authorization.
    - Former county child support investigator had **used a computer to improperly access** driver's license data of more than 370 county residents over four years.
    - Alleged violation of the federal Driver's Privacy Protection Act.
    - Plaintiffs claimed the County "failed to put into place systems and/or procedures to ensure … private data would be protected and would not be subject to misuse."

Source: *Gulsvig v. Peterick*, No. 13-CV-01309 (D. Minn.) (various pleadings and court filings)

Examples of Insider Threats

- **State Government Laptops Stolen from Car**
  - Midwestern State Revenue Department announced in July 2016 that it was notifying nearly 1,000 taxpayers whose personal information was on one of four laptops stolen from a rental car in San Francisco.
    - The department said that **some procedures to secure data may not have been followed with one laptop**, but that its network had not been accessed or hacked.
    - Revenue Department paying for one year of credit monitoring for individuals affected by the data loss.

Source: Pennsylvania Department of Revenue Press Release, July 12, 2016

Understanding the Threats: *Outsiders*

- **Hackers**
  - Activists
  - Nation-state actors
- **Malware**
  - Including ransomware
- **Phishing**
  - Including spear-phishing, whaling, and SMiShing
- **Thieves**
- **Vendors**

Examples of Outsider Threats

- **Hack Costs Arizona County Community College District $26 million**
  - In May 2016, an Arizona county community college district finally settled a class action stemming from a massive data breach in 2013.
    - FBI notified the community college in 2013 that **hackers had breached the district's systems**, resulting in the theft of SSNs and other sensitive personal information of more than 2 million employees, students, and applicants.
    - District's governing board had approved **$26 million** to deal with the breach:
      - $9.3 million in legal fees
      - $7.5 million in cyber consulting fees and network repairs and upgrades
      - $7.0 million for notifications and credit monitoring
      - $2.2 million for records management, public relations, and photocopying

Sources: -Various docket entries in *Roberts v. Maricopa County Community College District*, No. 14-CV-02086 (D. Ariz.)
-Maricopa County Community College District Government Board Minutes

Examples of Outsider Threats

- **California County Breached by Overseas Hackers**
  - Personal information of nearly 150,000 California county residents exposed to foreign **hackers who tapped into county computer** in March 2013
    - Lost data included names, SSNs, addresses, and birth dates of county residents who had received state social service payments between 2002 and 2009.
    - The hacked computer **had not been used for four years**, but was left connected to a state government network that hackers used to gain access to the computer.
    - The county was forced to notify the affected individuals, as well as the California Attorney General's Office and the California State Office of Privacy Protection.

Source: Monterey County Department of Social Services Notification Letter, September 20, 2013

Examples of Outsider Threats

- **Massachusetts Town Victimized by Ransomware**
  - A Massachusetts town with fewer than 30,000 residents paid $600 to regain access to its records being held hostage by hackers in late 2014.
    - The hackers had, among other things, **disabled the town's emergency systems**, which added urgency to the situation.
    - After struggling for several days to unlock its systems, town officials decided they had no choice but to pay the ransom.
    - "We are so petrified we could be put into this position again. ***Everyone is vulnerable***."

Source: "Ransomware: Extortionist Hackers Borrow Customer Service Tactics," *Reuters*, April 12, 2016

Examples of Outsider Threats

- **California City Transportation Agency Hit with Ransomware**
  - A large California city's municipal transportation agency had its computer systems disrupted by a November 25, 2016 ransomware attack.
    - The hack reportedly **affected the agency's ticket-selling systems**, causing kiosk screens to display, "You Hacked, ALL Data Encrypted."
    - "As a precaution to minimize possible impacts to [its] customers," the agency disabled fare gates – **resulting in free rides for customers** – over the Thanksgiving weekend.
    - The hackers reportedly demanded $73,000 in ransom.

Source: "San Francisco Public Transit System Hit in Ransomware Attack," *Reuters,* November 28, 2016

Examples of Outsider Threats

- **Two State Voter Systems Breached in the Summer of 2016**
  - The FBI found breaches of **two states' voter registration databases** in the months leading up to the 2016 elections.
    - One state's voter registration system was shut down for more than a week in July after the hackers had **downloaded personal data on 200,000 voters**.
    - A second state was forced to shut down its election website in June after the introduction of malware into a state employee's computer.
    - Both breaches may have been overshadowed by the hacks of the Democratic National Committee and others in the Democratic Party, but the **threat to the electoral process** on the state level remains real.

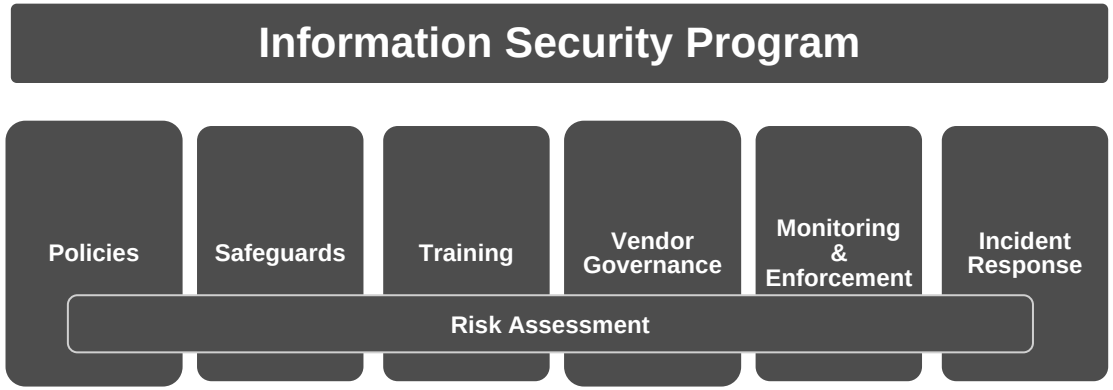
Sources: -"FBI Detects Breaches Against Two State Voter Systems," *Reuters,* August 29, 2016
-"Targeting Activity Against State Board of Election Systems," *FBI, Cyber Division Flash Alert*, August 18, 2016
-"Illinois Voter Registration System Database Breach Report," *Illinois State Board of Elections*, August 26, 2016.

The Role of Counsel in Preventing Data Breaches

What Counsel Can Do

Most data breaches and cyber incidents are preventable.
Counsel can help government entities minimize their risks and the potential impact of these unfortunate events.

- **Help the organization understand that these are not just IT issues.**
- **Develop a WISP and appropriate policies and training.**
- **Create and maintain data and IT asset inventories, because you cannot protect something that you don't know is there.**
- **Support regular risk assessments.**
- **Maintain sound safeguards, including vendor oversight and governance.**
- **Stay vigilant because privacy and data security laws (and risks) are constantly evolving.**
- **Prepare for the worst with a solid (and tested!) incident response plan.**

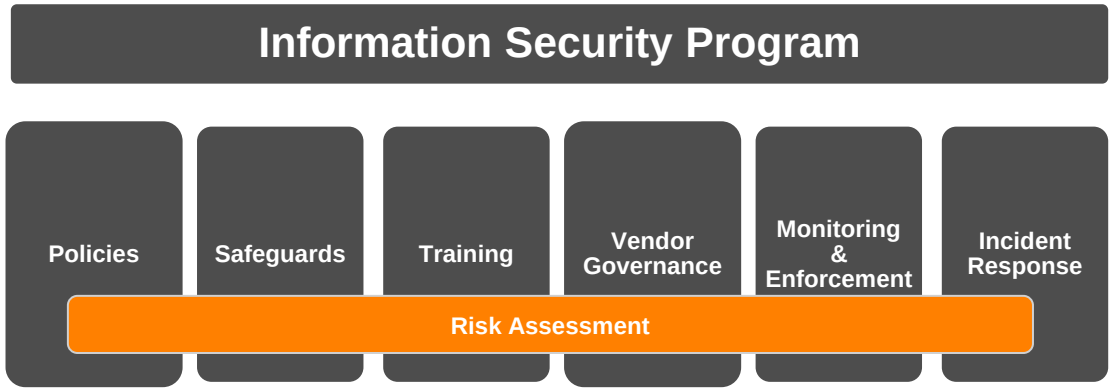


Counsel's Role in Data Security Risk Assessments

Risk assessments are inherently operational, but counsel plays an important role in this critical information security activity.

- **Risk assessments are explicitly required by**:
  - Some data security laws and regulations
  - Generally accepted industry standards
- **Other laws and regulations (and typical contracts) use a reasonableness standard.**
- **Organizations look to counsel for advice on what is reasonable.**

- **To provide effective advice, counsel must understand:**
  - Terminology
  - Processes
  - Standards

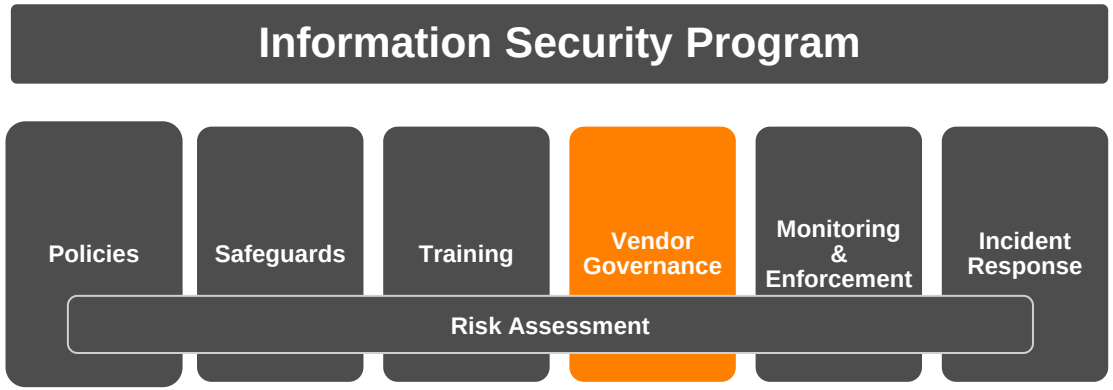


Vendor Governance

Engaging vendors to provide IT and data-related services changes an organization's information security risk profile.

- **Contract provisions**
  - Applicable laws
  - Standard of care for privacy and data security
  - Data uses and disclosures
  - Subcontractors
  - Service level agreements (SLAs)
  - Return or destroy data
  - Incident reporting and response
  - Audits and oversight methods
  - Risk management and cost allocation

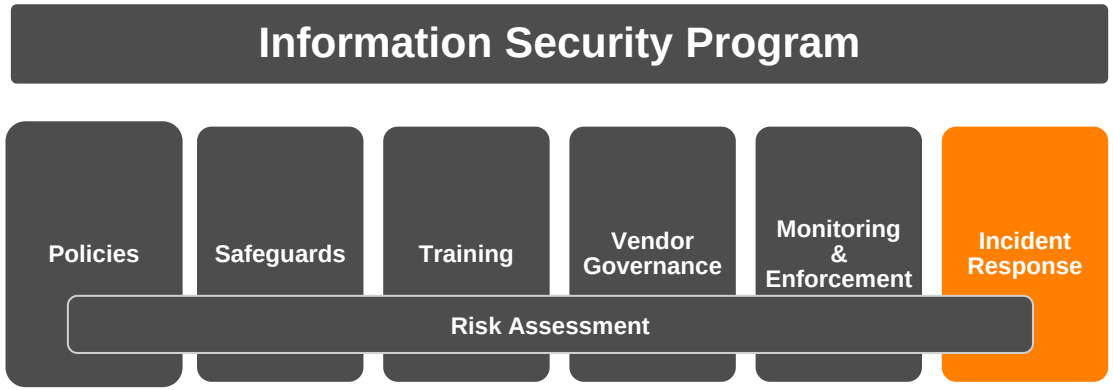
- **Key program elements**
  - Vendor tracking and approval
  - Pre-engagement due diligence
  - Standard contract provisions
  - Oversight and enforcement



Incident Response Plan

- **A written incident response plan should identify data breach scenarios and set out appropriate responses.**
  - Required by certain state and federal laws
- **Customized for your organization's particular circumstances, but should generally include basic components:**
  - Clear leadership and accountability
  - Response team
  - Incident discovery and reporting
  - Initial response and investigation
  - Recovery and follow-up
  - Public relations
  - Law enforcement

- **Teams typically include representatives from:**
  - Legal
  - Data or privacy office, or both
  - IT and information security
  - Human resources
  - Affected agency or units
  - Audit
  - Public relations or media relations



Incident Response Preparation and Testing

- A little planning goes a long way.
- Response preparation and planning should include:
  - Internal communications and escalation paths
  - Legal analysis for data breach notification obligations
  - Example notification letters
  - Pre-negotiated service provider agreements
    - Computer forensics investigators
    - Affected individual notifications
    - Credit protection and monitoring (if applicable)
  - Law enforcement contacts and engagement criteria
- **TEST, TEST, TEST** with real-life scenarios and stakeholder engagement.

Relevant Practical Law Resources

- **Practice Notes**
  - *Cyber Attacks: Prevention and Proactive Responses*
  - *Breach Notification*
  - *The NIST Cybersecurity Framework*
  - *Data Security Risk Assessments and Reporting*
  - *Managing Privacy and Data Security Risks in Vendor Relationships*
- **Standard Documents**
  - *Data Security Breach Notice Letter*
  - *Information Security Policy*
  - *Written Information Security Program (WISP)*
- **Checklists**
  - *Data Breach Response Checklist*
  - *Common Gaps in Information Security Compliance Checklist*
  - *Performing Data Security Risk Assessments Checklist*
- ***Data Breach Notification Laws*: State Q&A Tool**

CLE Credit

CLE credit is available for: Arizona, California, Colorado, Georgia, Hawaii, Illinois, Indiana, Mississippi, Missouri, New Hampshire, New Jersey, New York, North Carolina, Pennsylvania, Vermont, Washington.

CLE credit is being sought for: Louisiana, Minnesota, Oregon, Tennessee, Texas, Virginia

CLE credit can be self-applied for in: Florida

To obtain your certificate of attendance for your use in CLE credit compliance, please fill out and submit the online form:

https://wlec.formstack.com/forms/pl_219572

Once we receive your request, we will process it within an average of two (2) weeks. **Your certificate will be archived on www.westlegaledcenter.com and instructions will be e-mailed to you on how to download your certificate from this location for your own records.**

If your requested state(s) allow the sponsor to report your CLE attendance, we will do so and pay the associated fees within 30 days of your course.

If you have questions, please contact accreditation@westlegaledcenter.com.