CCISDA

California Counties Information Services Directors Association

California Counties Information Security Programs

A look into the progress and future plans across counties

2010 Progress Report

April 2010

Table of contents

Keeping California Running and Growing: **3**
A Message From the ISF Officers

A Look Inside the Information Security Forum
Best practices information security program **4**
Summary of survey responses **5**

Information Security Program and Awareness Progress Survey Results
Workforce training **6**
Data classification **7**
Security controls **8**
Monitoring and auditing **9**
Policy and procedures **10**
BCP / DR **11**
Risk management **12**
Security professionals **13**
Governance **14**

CCISDA Information Security Forum
2010 hot topics **15**
Recent Accomplishments **16**

Acknowledgements **17**

Information security program progress survey **18**

CCISDA Information Security Forum Charter **20**

Keeping California Running and Growing

Welcome to our first edition of the California Counties Information Security Program Progress Report.

In January 2010 we surveyed 52 attendees at the all-day C California Counties Information Security Forum (ISF) held in Sacramento. Attendees represented 21 of the 58 counties which is 38% of the total.

I've been encouraged by the successful operations and level of sophistication within many of our counties.

Yet as we struggle with protecting our information assets, it is imperative that we leverage opportunities to meet our technology and security needs.

A first step is to inventory where we are.

Gathering this information will let us take advantage of economies of scale and progress our peers are making.

To get to the bottom line of the progress we are collectively making in security programs we developed a survey.

The survey gathered data across the nine components of an information security program.

This input is extremely important in capturing a big picture view of our county security programs and guide our CCISDA ISF information security policies and strategies.

We look forward to working closely with CCISDA and the ISF to coordinate the direction of information security within California's counties.

Jim Reiner
ISF Chair
Sacramento County
916-874-6788

Scott Cambridge
ISF Vice-Chair
El Dorado County
530-621-5151

From the ISF Charter:

ISF Purpose Statement:

- to create standards documents for state-wide use;
- to serve as a technical resource to the greater CCISDA organization;
- to serve as a collaborative Forum to disseminate security-related information from various sources; and
- to promote security awareness and education.

Best Practice Information Security Program

From the California Counties "Best Practices" Information Security Program – Adopted by CCISDA March 2002

This document outlines an Information Security Program based upon industry and governmental proven "best practices," and designed for adoption by California Counties accepting the above-noted challenges.

This program was developed under the auspices of the California County Information Services Directors Association (CCISDA), which chartered an Information Security Forum (ISF) to discuss, define and develop the recommendations made in this document and model those proven to be best practices.

The CCISDA ISF consists of information security professionals employed by counties across California.

CCISDA encourages all members to adopt information security best practices.

Because this document is based on best practices and written by county staff, it can provide a firm foundation for establishing an effective information security program in any county.

It is expected that every California county will benefit directly from a best practices program, and will implement this program to protect its information systems and ensure continuity of government services.

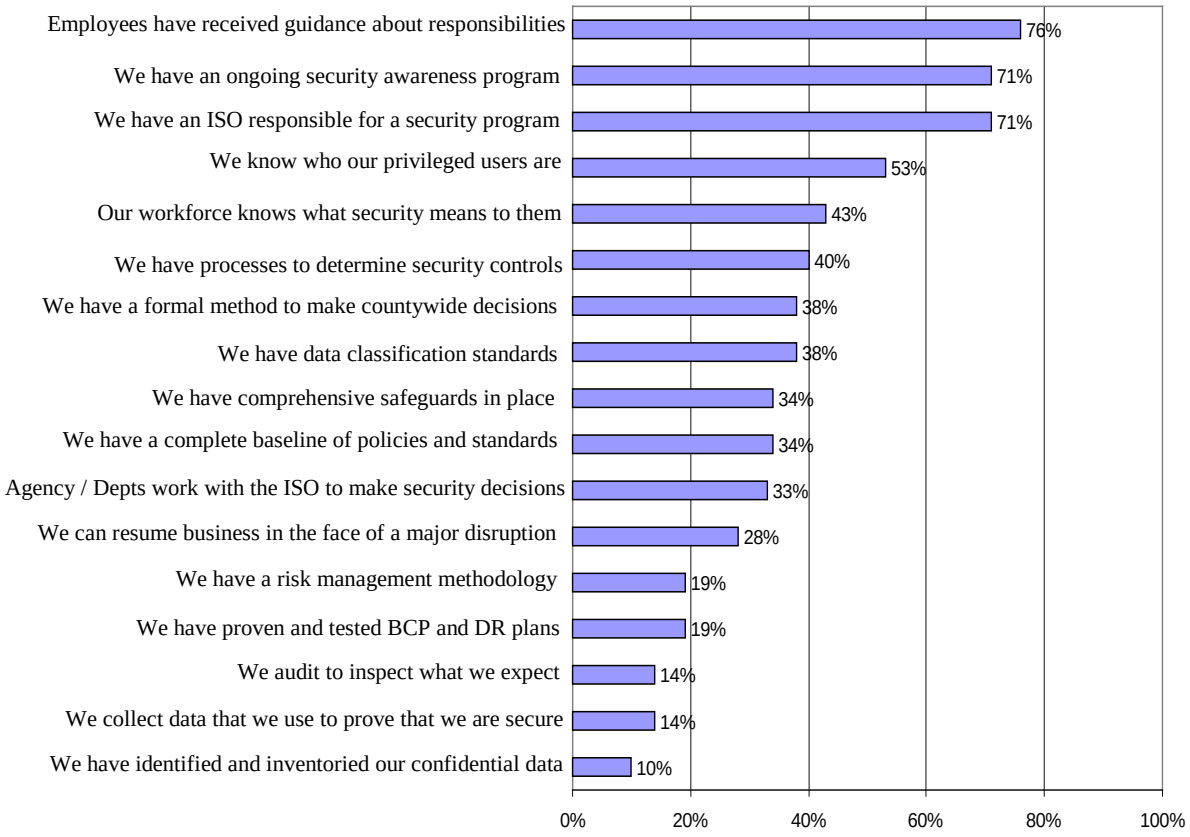
It is recommended that all California Counties implement this Best Practices Information Security Program through a Board of Supervisors resolution.

The nine components of an information security program

- Governance
- Security Professionals
- Employee Training and Awareness
- Security Controls
- Information Classification
- Monitoring and Auditing
- Policy and Procedures
- BCP / DR
- Information Risk Management

Note: The following survey results are based on these components of a best practices information security program. The survey itself is on pages 18 and 19.

Survey responses ranked by most favorable



- The survey results indicate that counties focus on different aspects of security.
- Counties taken as a whole are still maturing their programs. For every aspect of security where many are still ramping up, there are some that have made great progress. Therefore, we can learn from each other.
- Recommend targeting four issues for special action: risk management, regulations and compliance, continuity planning and disaster recovery, and governance. Each of these requires some amount of business/program involvement for success.
- Recommend using the survey results to identify other areas for improvement strategies.

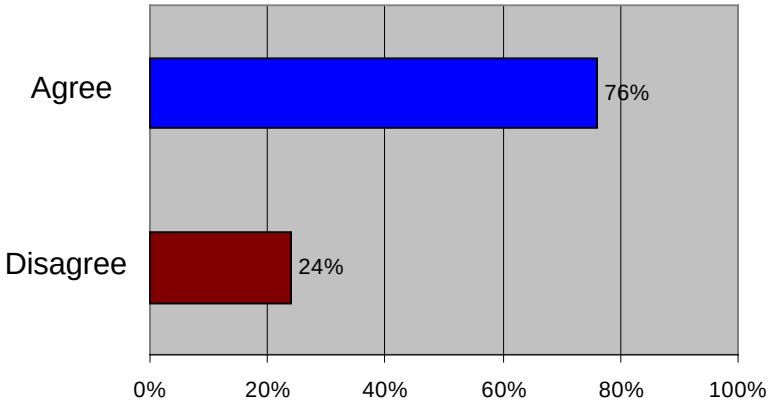
Workforce Training

For any set of policies to work, the target audience must be aware of it and understand it.

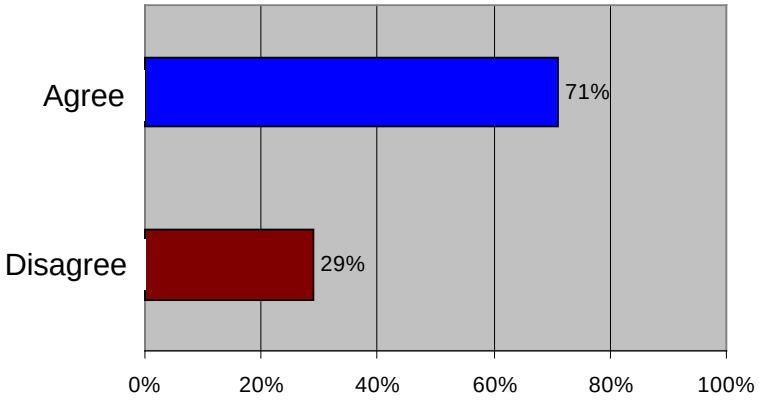
Observations

- Ongoing outreach and awareness is critical.
- 76% of counties indicate that employees receive guidance, but at the same time 57% don't think the workforce knows what it means to them.
- This is the area with the overall highest favorable rating. Counties recognize the value in this effort.

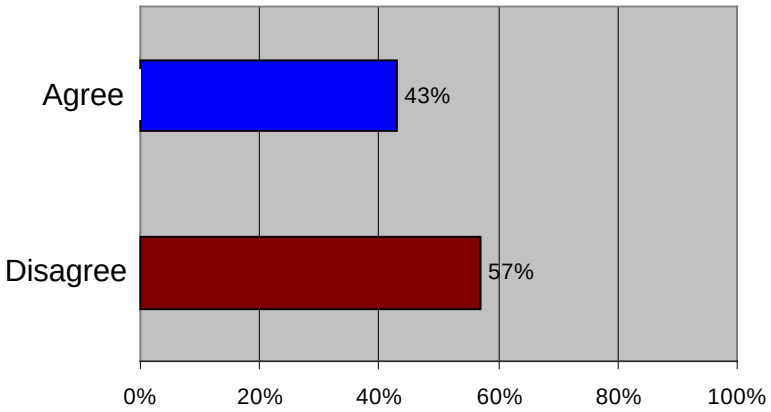
1a) Employees receive guidance about measures and actions that they are responsible for.



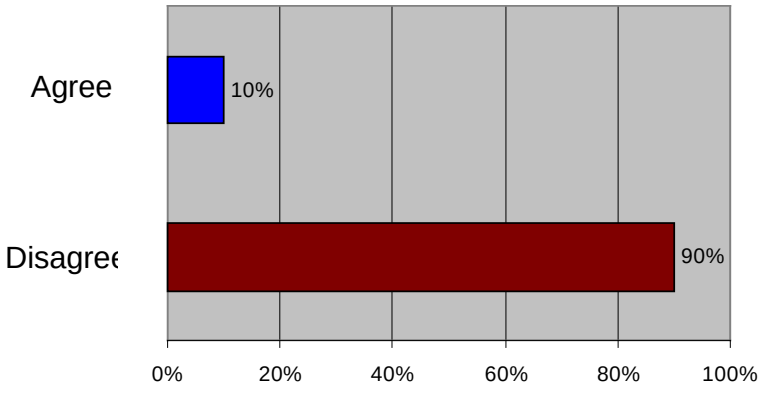
1b) We have an ongoing information security awareness program for the workforce.



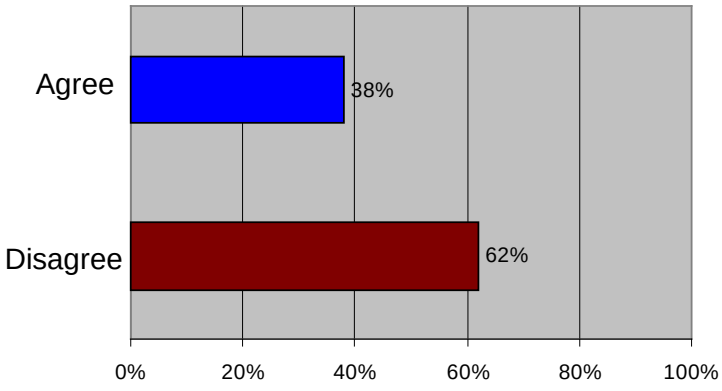
1c) Workforce knows why we have a program and what it means to them.



2a) We've inventoried and identified all our confidential data.



2b) We have standards by which information resources are managed and accessed.



Data Classification

A classification scheme is used to determine adequate and appropriate procedures, and their associated access controls.

Observations

- This is the least mature area in information security programs.
- It is extremely difficult to put in place risk-based security controls if you don't know what you are trying to protect or where it is.

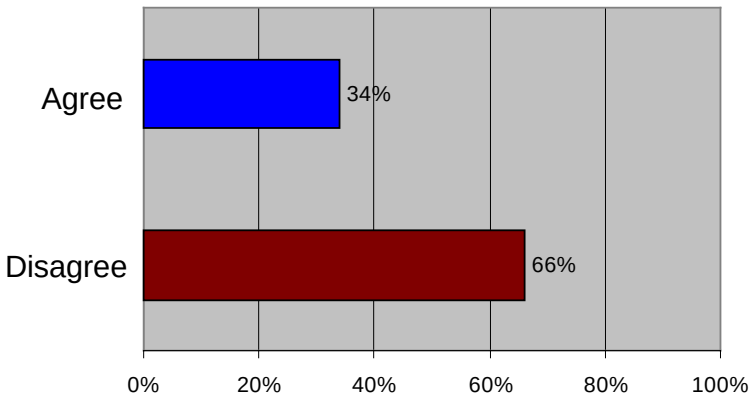
Security Controls

Implementing security controls focuses on the generalized mechanisms that control access to data and resources.

Observations

- There is a story behind the data. The weak spot in many organizations is the lack of administrative controls – countywide policies.
- While many organizations are better with the technical controls, there is still a gap in implementing these controls based on risk assessments.
- Physical security is often not on the radar and needs to be elevated as well.

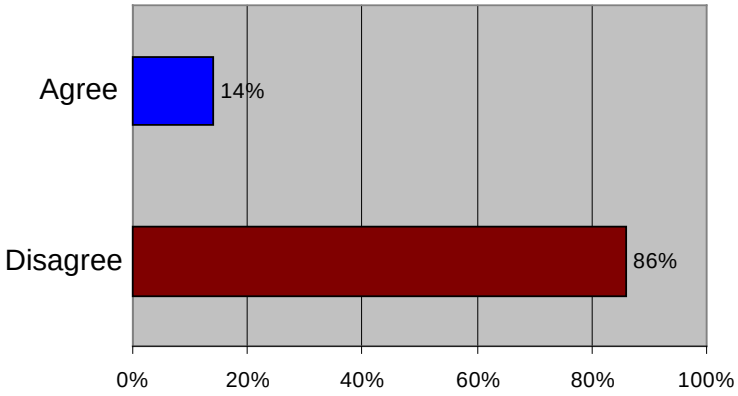
3 We have comprehensive controls in place: admin, physical, & technical.



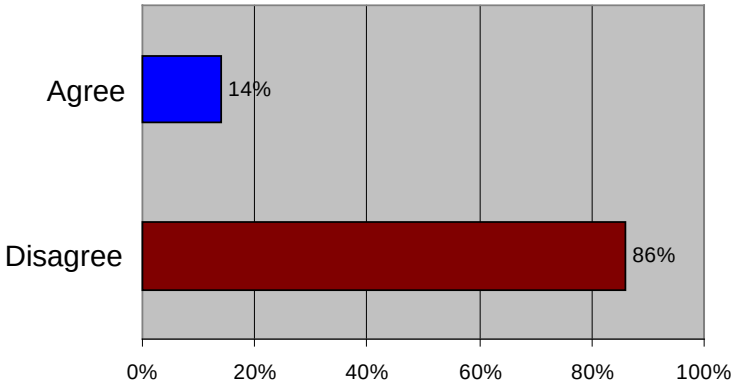
Monitor and Auditing

Monitoring effectiveness and assurance is an integral part of a good Information Security Program, enabling the county to demonstrate value and provide reassurance.

4a) We inspect what we expect for compliance with standards.



4b) We collect data that we use to prove that we are secure.



Observations

- The data shows we are quite immature overall in monitoring and compliance.
- This puts us at risk in that we really don't know what our county risk profile is.
- In the absence of data to substantiate that we are secure, many of us are guessing or ignoring it.
- We tend to be reactive and not using a proactive risk management methodology.

Policy & Procedure

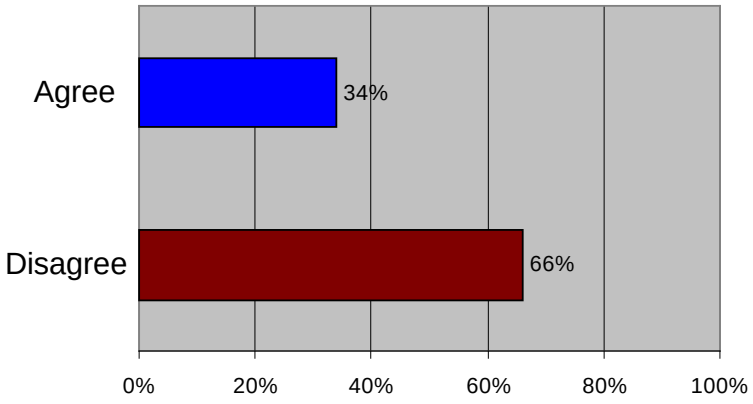
The first step in establishing an effective Information Security Program is to document the policies (decisions) for protecting information.

Policies provide guidance for users, administrators and managers to protect information.

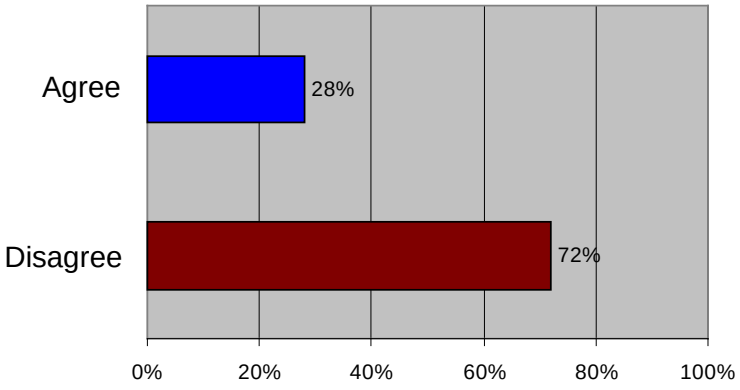
Observations

- The majority would characterize their policies as incomplete.
- While most counties have some security policies, these were often in reaction to incidents or court cases.
- Only a holistic approach based on an industry standard provides a policy benchmark.
- Counties would benefit from a gap analysis and a risk analysis to determine policy needs.

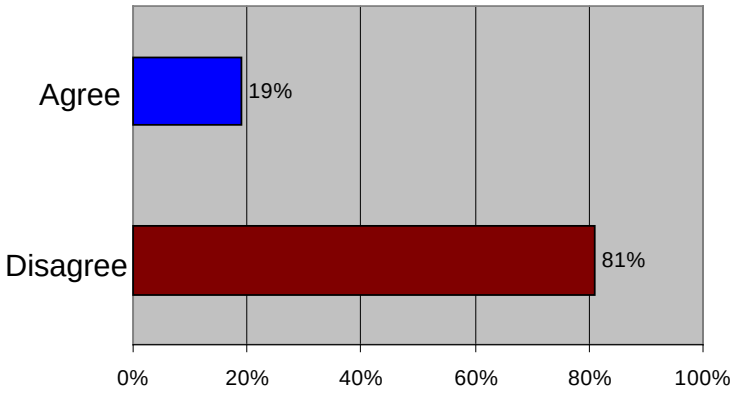
5 We have a complete baseline of security policies and standards.



6a) We can run our business in the face of major disruptions



6b) We have a proven and tested plan to resume work with employees, vendors, and customers



Business Continuity & Disaster Recovery

All government agencies need to be prepared to deal with business disruptions and have a plan to resume business processes.

Observations

- Most counties focus on backup and restore capabilities of the technical components.
- There is a major disconnect with the business side.
- If business does not conduct a risk assessment, then IT can only restore technical components, not the actual business processes themselves.

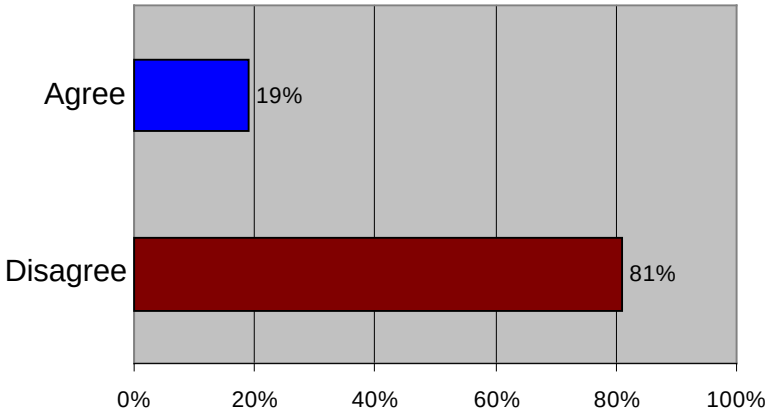
Risk Management

Managing information risk: how to identify, analyze, and ultimately make well informed decisions that will more than likely contribute to the success of the county business.

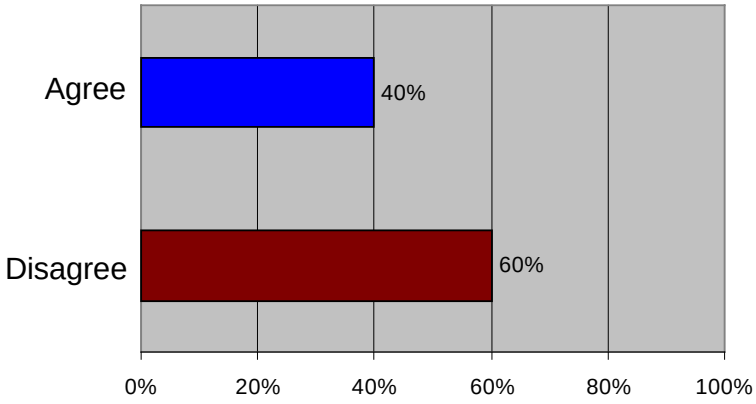
Observations

- This is an area where counties are not very mature.
- Managing risk is fundamental to policy and standards decisions.
- In the absence of a risk management methodology – a repeatable process with consistent outcomes – how do we know if our controls are right, if our policy decisions are right, if our data is secure? We don't.
- Business and IT must engage on this together.

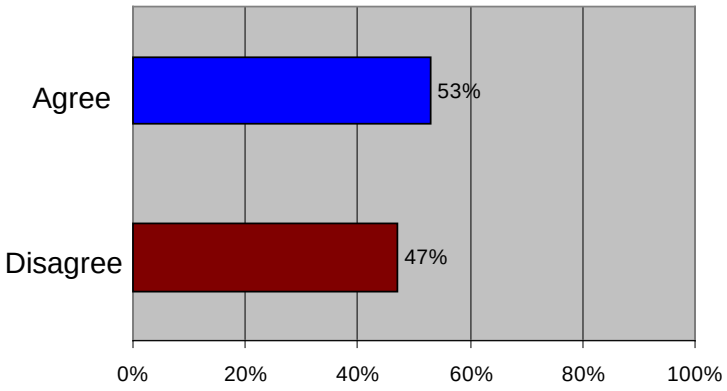
7a) We have an ongoing risk management methodology.



7b) We have a formal analysis process to determine security controls for business.



8 We know who are privileged IT users are, we train them, & they sign a confidentiality agreement.



Security Professionals

Security professionals implement and sustain the security controls and processes.

Observations

- Counties are almost evenly split on this.
- Just like identifying information assets to protect, we need to identify people with special access rights and understand the controls needed to securely manage them.

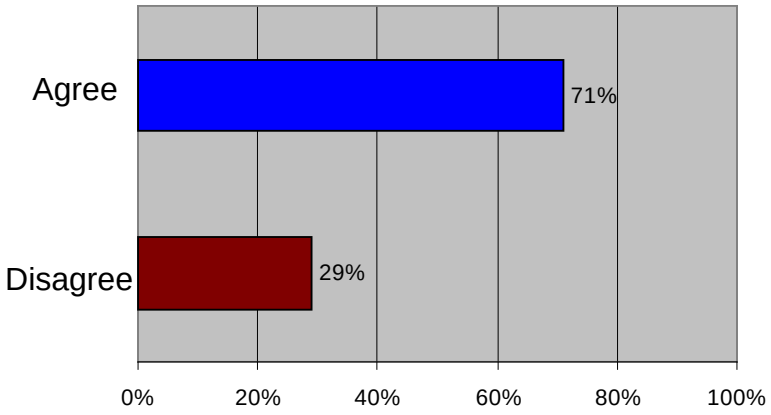
Governance

Departmental representatives, in conjunction with the Chief Information Security Officer, review and update the Information Security Program and associated policies as necessary to ensure that the policies enable county agencies to accomplish their objectives.

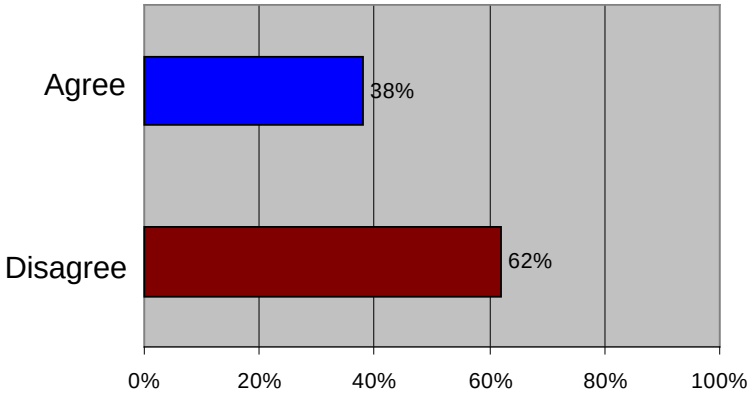
Observations

- 71% of counties have appointed someone as their ISO responsible for the security program.
- However, the business side is missing from the program implementation in almost 2/3 of the counties.
- This is the foundation. Business and IT must be at the table together making decisions about securing assets.

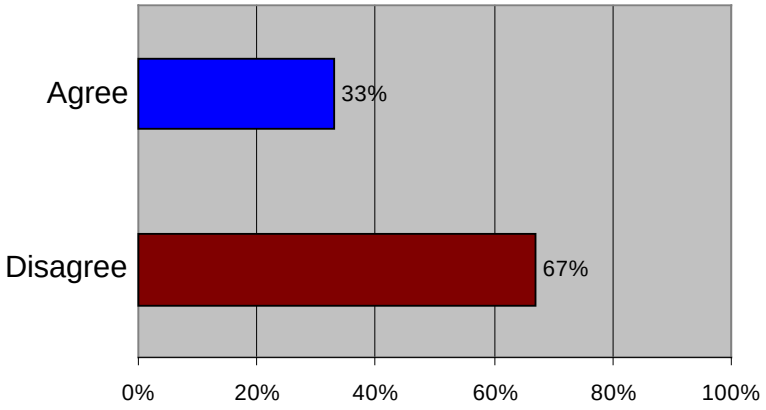
9a) We have an ISO responsible to develop and enforce a program.



9b) We have a formal method to make countywide security decisions.



9c) Agency / Dept representatives work with the ISO to manage the security program.



CCISDA ISF

2010 ISF Hot Topics

These focus areas and objectives are the basis for our 2010 efforts.

How do you get a risk management program going?

- learn how to work with business units to assess risk
- collect benchmarking data for comparisons between counties
- find good methods for presenting findings from a risk assessment

How can you possibly maintain security with social media?

- learn how to enable social media while staying secure
- collect and/or develop best practice policies for use of social media
- understand risk management tools and techniques for this area

How do you maintain end user awareness of information security practices?

- find solutions to awareness training for the workforce
- get leads for grant money that could be used to fund this
- get involved in whatever solution the State Security Office may be putting together

What do I need to know about regulations and compliance?

- inventory & build a reference document of regulations that apply to counties
- identify tools and techniques for tracking and evaluating compliance
- develop models to understand governance, risk, and compliance

Three Year Progress Update

Some of the topics that the ISF covered the last 3 years:

Security controls survey
Metrics
E-discovery
Application and Data Base Security
PKI
Program success
ISO 17799 Audit
MS-ISAC
Strategy to adopt a security program
Portable Device Encryption
Remote access
BCP
Awareness training
Security challenges
Most important security question
Communicating the business case
Incident management
Cyberstorm
Data exchange with the State of CA
Identity access management
Network vulnerability assessment
Centralized vs decentralized
Tips for the ISO
Policy refresh for ISO 27002
Collaboration across jurisdictions
Risk management
Single sign on
Disaster recovery

Recent ISF Topics / Presentations

November 4, 2008 CCISDA Fall Conference
- Adopting a county information strategic plan
- ISF workgroup initiatives: security policies, application security, metrics, training and education

January 27, 2009, Full Day Meeting
- Data exchange agreements between jurisdictions
- DHS training and grant opportunities
- Email security solutions
- Implementing disaster recovery solutions
- Application security questions
- Information classification case study

April 19, 2009 CCISDA Spring Conference
- Adopting a risk-base information security policy and program

July 22, 2009 ISF Full Day Meeting
- Update on President's Cyber Security Report
- Remote access and mobile computing
- End point protection solutions
- HITECH, FACTA, Red Flags
- Implementing vulnerability assessment tools
- State Security Office: new policies

Sept 27, 2009 CCISDA Fall Conference
- Information Security Legislation and Compliance
- Risk management

January 20, 2010 ISF Full Day Meeting
- Implementing Single Sign-On
- Adopting the ISF charter
- Developing a County risk profile
- Update on LA's cloud computing initiative
- Preparing for the Hi-Tech Act
- Process improvements with counties and DMV
- State Security Office: CA Security Strategic Plan

April 25, 2010 CCISDA Spring Conference
- County infosec program progress report
- Workgroup reports: social media, compliance, risk management, training, peer survey

The last seven ISF events each drew over 50 attendees from as many as 35 different counties.

Attendees benefit from prepared presentations, briefings, and open forum opportunities for information sharing and collaboration.

Acknowledgements

The authors wish to thank their colleagues who completed the Information Security Program questionnaire and those who reviewed working drafts of this document.

The 21 organizations and 52 staff who attended the January 20, 2010 Forum are to be recognized for their efforts.

And it is fitting to acknowledge the members that have been active participants since the ISF formed in 2000. Their continual support is invaluable.

In addition, we are grateful for the speakers, sponsors, and last but not least the continual support of the ISF by the CIOs of the counties in the state of California.

Are we making progress as leaders?

Your perception as a leader is important to our organization. For each statement, check the box that best matches how you feel. How you feel will help us decide where and if we need to improve. Answer from a countywide perspective.

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
CATEGORY 1: Workforce Training					
a) Employees receive information privacy and security guidance regarding protective measures and actions they are responsible for.	☐	☐	☐	☐	☐
b) We have an ongoing information security awareness program for the workforce.	☐	☐	☐	☐	☐
c) Our workforce knows why we have a security program or what it means to them.	☐	☐	☐	☐	☐
CATEGORY 2: Data Classification	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We've inventoried and identified all confidential data assets that need special controls for access, use, disclosure, and disposal.	☐	☐	☐	☐	☐
b) We have standards by which information resources are managed and accessed.	☐	☐	☐	☐	☐
CATEGORY 3: Security Controls	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We have comprehensive and consistent safeguards in place: administrative, physical and technical safeguards to protect information assets.	☐	☐	☐	☐	☐
CATEGORY 4: Monitor and Audit	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We inspect what we expect for compliance with security standards.	☐	☐	☐	☐	☐
b) I can confidently answer <u>with data</u> that I know I am secure.	☐	☐	☐	☐	☐
CATEGORY 5: Policy and Procedure	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We have a complete baseline security standard and have documented our decisions about expected behavior and system security.	☐	☐	☐	☐	☐

CATEGORY 6: BCP / DR

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We can preserve our business in the face of major disruptions.	☐	☐	☐	☐	☐
b) We have a proven and tested plan for resuming work with employees, customers, and vendors.	☐	☐	☐	☐	☐

CATEGORY 7: Risk Management

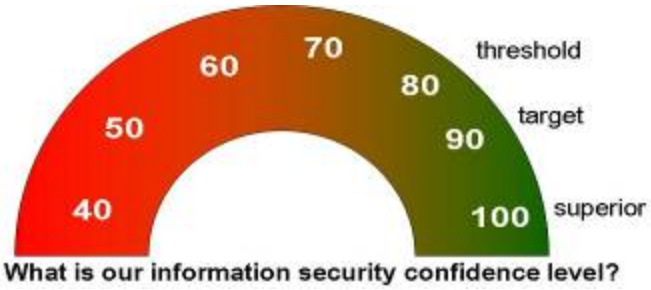
	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We have an ongoing risk management methodology: a repeatable process with consistent results to classify risk and impact – financial cost and constituent confidence.	☐	☐	☐	☐	☐
b) We have formal analysis process to determine reasonable and appropriate security controls for the business.	☐	☐	☐	☐	☐

CATEGORY 8: Security Professionals

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We know who our privileged IT users are, train them, and they sign a confidentiality agreement.	☐	☐	☐	☐	☐

CATEGORY 9: Governance:

	Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
a) We have an information security officer responsible to develop and enforce the security program.	☐	☐	☐	☐	☐
b) We have a formal method to make countywide decisions about business risks, impact, priority, policy, and minimum standards.	☐	☐	☐	☐	☐
c) Agency representatives work with the ISO to review and update the information security program and policies as necessary.	☐	☐	☐	☐	☐



What is our information security confidence level?

Information Security Forum Charter

1.0 Information Security Forum Governance (defined):

Information Security Forum (Forum) governance is criteria that guide how the Forum manages its operation. The Forum is a subordinate working committee to CCISDA, and its board members provide oversight to the Forum participants.

2.0 Information Security Forum Purpose Statement:

To create standards documents for state-wide use; to serve as a technical resource to the greater CCISDA organization; to serve as a collaborative Forum to disseminate security-related information from various sources; and to promote security awareness and education.

3.0 Guiding Principles:

The Forum members will conduct business in an environment that expects:

- Honesty
- Timeliness
- Open, and respectful communication
- Informed decisions that acknowledge unique needs of each county
- Considers what is best for the entire CCISDA organization.

4.0 Information Security Forum Participant Requirements & Responsibilities:

The Forum is open to employees of any California County technology support team interested in and/or involved with security implementation, as authorized by the County CIO / IT Director, or the County Chief Information Security Officer (CISO) / IT Security Manager. All attendees are expected to support the Forum's purpose and participate and contribute to the extent possible in Forum initiatives.

5.0 Forum Procedures:

A. Communications:
   - All meetings will have agendas provided, and meeting notes or a summary will be published electronically to the Forum E-mail distribution list. It is intended that meeting agendas will place priority on issue resolution and on decision making rather than status reporting.
   - A roster of members will be maintained by the officers of the Forum and be distributed to all participants at least annually.

B. Meetings:
   - The Forum will typically meet at least quarterly in person. Meetings typically will take place in the Spring and Fall as a CCISDA event break-out session. Winter and Summer sessions will generally be held as an all-day event.
   - The focus of meetings will be to discuss the major agenda item(s), make collaborative decisions, and endorse recommendations related to scheduled agenda items.

C. Voting
   - Items brought to vote at the Forum or electronically will generally be limited to one vote per participating County; however, everyone is encouraged to participate in the discussion and vetting of items. The County's representative that holds the highest-level job position/classification will determine that county's single vote. However, collaboration within that county can occur prior to that single vote being provided.

D. Officers
   - The Forum desires to stimulate personal and career growth and to develop leaders for tomorrow. As such, officers are selected for one year terms with the opportunity to continue participation or change responsibility each election cycle.
   - Elections are generally held during the Winter all day Forum session. New officers take effect immediately. Nominations may be gathered / accepted in the period between the Fall CCISDA and the Winter session.
   - Chairperson: Serves a one year term. The chairperson will finalize the meeting's agenda; establish the venue; review the meeting notes; responsible to disseminate the agenda and meeting notes to the participants; conducts the meetings; delegates assignments and projects; and provides communication and acts as liaison to the CCISDA board members during the semi-annual CCISDA events, and in off-cycle business meetings.
   - Vice-Chair: Serves a one year term; will serve as chairperson in the absence of the elected chairperson; acts as scribe at Forum meetings and submits the meeting notes to the Chairperson for review within two weeks after the meeting; coordinates the dissemination of the meeting notes with the Chairperson; and assists the chairperson in reaching the goals of the Forum's primary and other responsibilities.
   - Chairperson Emeritus: past Chairpersons who are still county employees can participate for life with this title and provide general guidance and advice to the other officers; can serve in any other capacity as needed.

E. Other Responsibilities of the Forum (generally the Chairperson or their delegate)
   - Participates as the California local government representative to the State on Information Security issues requiring / requesting partnering with local government.
   - Team member of the California delegation for the Multi-State Information Sharing and Analysis Center (MS-ISAC). This requires participation in the annual meeting as part of the California delegation (funded in full by the MS-ISAC), monthly teleconference calls, and expected to be a member of a work group.
   - Plan the annual Partner in Learning (PIL) Government Technology Conference (GTC) held in Sacramento each May in cooperation with State, City and County attendees. This is a collaborative meeting to focus on common best practices.
   - Receive and forward general Information Security advisories to the Forum E-mail list.
   - Participate in the bi-monthly State Information Security Officer's meetings in Sacramento as the local government representative.

6.0 Adoption

The adoption of this charter is constituted by review and approval from the Forum and the CCISDA Board of Directors.

7.0 Sunset Review

Upon adoption of this Charter, a review should occur every two (2) years commencing from the identified adoption/sunset date. This will ensure consistency as it applies to the CCISDA mission, goals, and objectives.

8.0 Authority

The CCISDA Executive Board of Directors approved this charter at their meeting held December 3, 2009.

California Counties Information Services Directors Association

CCISDA 2010 executive board

President
Gregg Jacob, Tuolumne County

First Vice President
Kevin Bowling, Santa Cruz County

Second Vice President
Joyce Wing, Santa Clara County

Secretary/Treasurer
Harold Tuck, San Diego County

Past President
Howard Stohlman, Calaveras County

www.ccisda.org