Mobile Security

Western Michigan ISACA

Sajay Rai, CPA, CISSP, CISM
President and CEO, Securely Yours LLC
sajayrai@securelyyoursllc.com

October 30, 2013

Agenda

- Security Smart Devices
- Security Features in iOS and Android
- Use of Mobile Devices in DR, IR and CM

Securing Smart Devices

Agenda

- Evolution of Smart Device usage
- 10 Steps
- Case Study

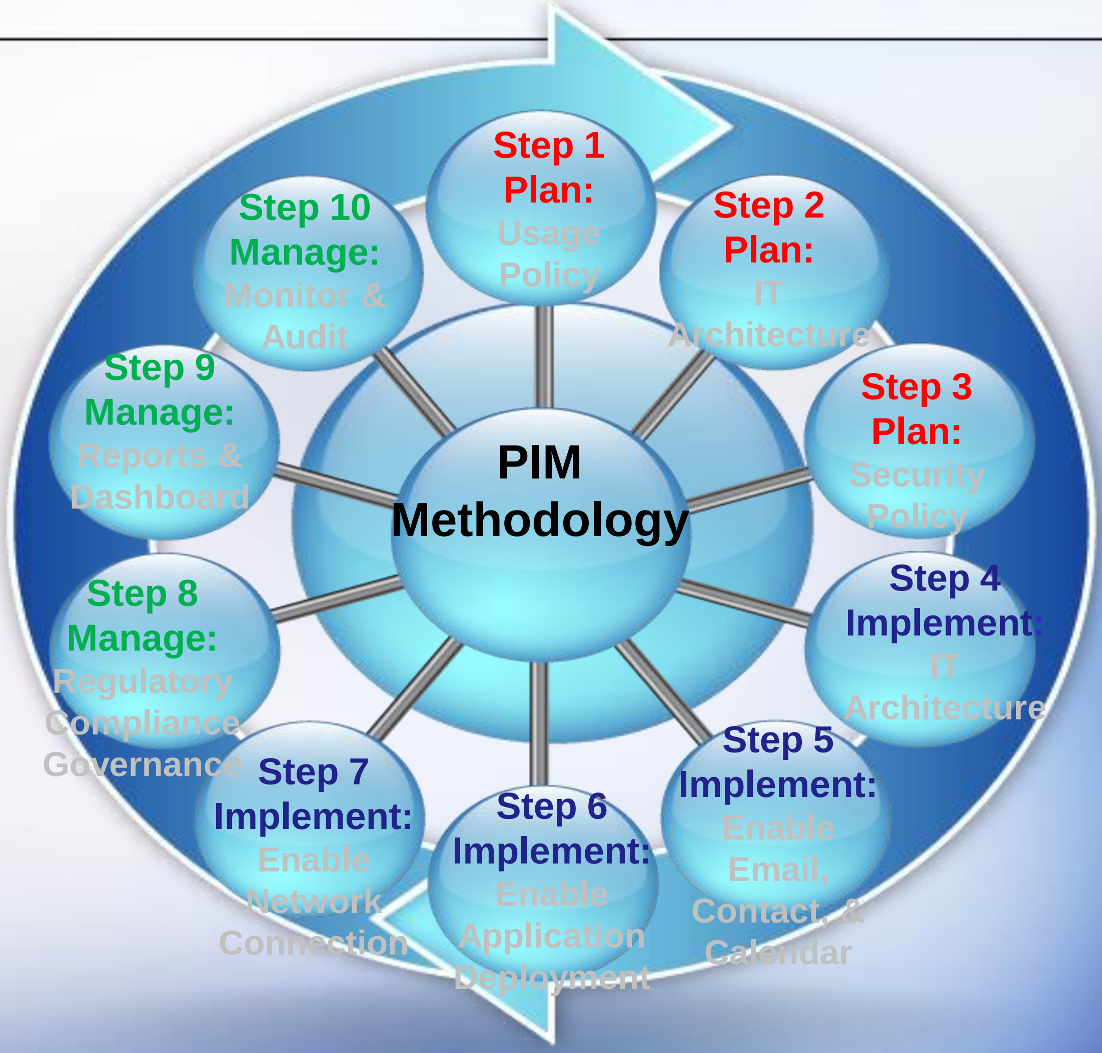
Evolution

It is projected that Android and iOS will be the leading operating system for smart devices from 2012 on.

- Most Organizations relied on blackberry
- iPhone and iPad changed the executive landscape
- IT under pressure to also support
  - – iOS (Apple)
  - – Android (Google)
  - – Windows Mobile (Microsoft)

Ten Steps

PIM (Plan, Implement, Manage) methodology provides a comprehensive approach to organizations to manage and secure the smart devices.



PIM Methodology

Step 1 Plan: Usage Policy

Step 2 Plan: IT Architecture

Step 3 Plan: Security Policy

Step 4 Implement: IT Architecture

Step 5 Implement: Enable Email, Contact, & Calendar

Step 6 Implement: Enable Application Deployment

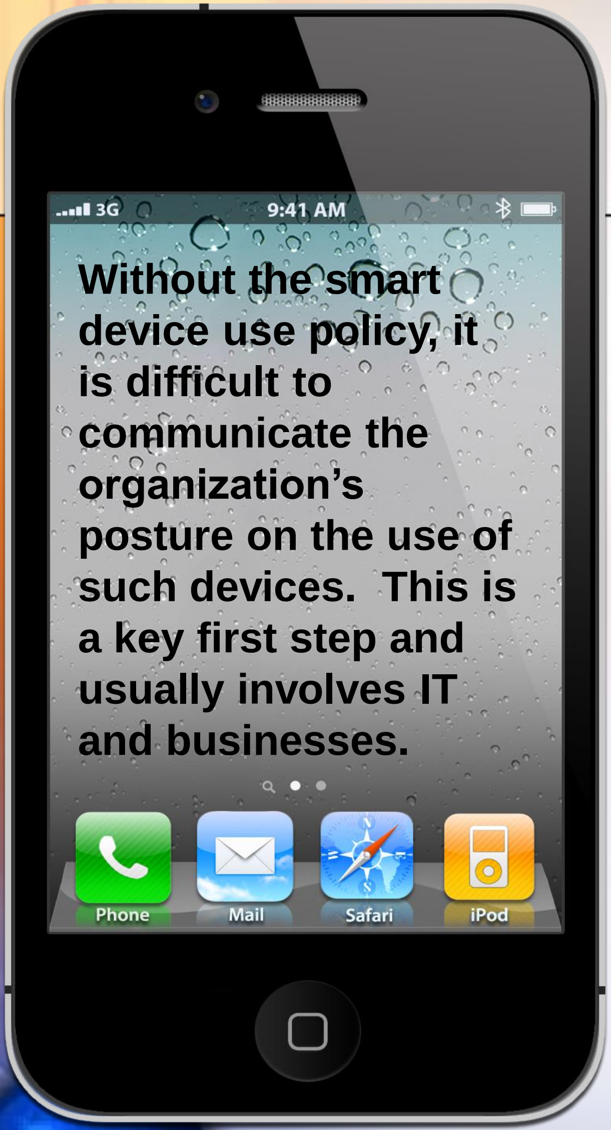
Step 7 Implement: Enable Network Connection

Step 8 Manage: Regulatory Compliance Governance

Step 9 Manage: Reports & Dashboard

Step 10 Manage: Monitor & Audit

Step 1



Without the smart device use policy, it is difficult to communicate the organization's posture on the use of such devices. This is a key first step and usually involves IT and businesses.

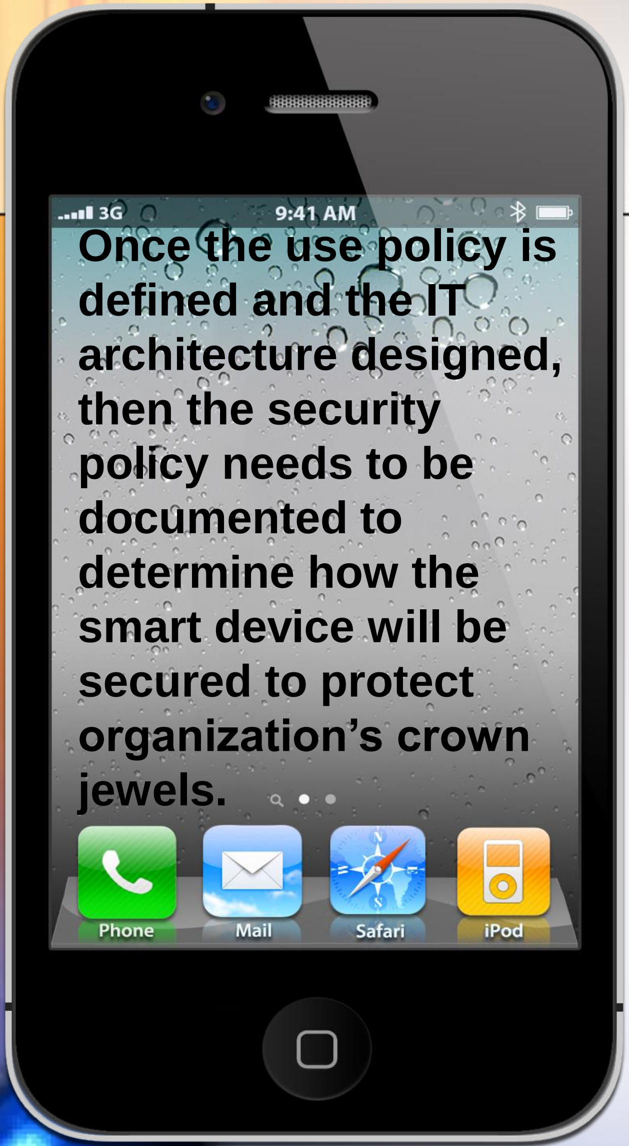
- Step 1: Define the smart device use policy. Consider the following:
  - Corporate devices vs. employee devices
  - Separation of personal vs. corporate data on device
  - Personal use or only corporate use? Can you play Angry Bird on your device?
  - Agreement with employee to abide with corporate security policies (e.g. remote wipe, or record of their phone calls may be viewed by corporate)
  - Would confidential data be allowed on smart devices and how it will be monitored and controlled?
  - What type of smart devices will be allowed? Apple only? Android only? Or limit by operating systems?
  - How are you going to manage the backup?
  - Would you want the device to connect to corporate network?
  - Which apps would you like to deploy? Corporate apps? Own Marketplace?

Step 2

Once it is known how the smart devices will be used, designing the supporting IT architecture is the logical next step. This architecture maps to the existing IT architecture.

- Step 2: Design the smart device IT architecture. Consider the following:
  - – Cloud based solution vs. internally deployed
  - – Hosted vs. self supported
  - – Number of devices supported and scalability
  - – Changes to the current IT architecture

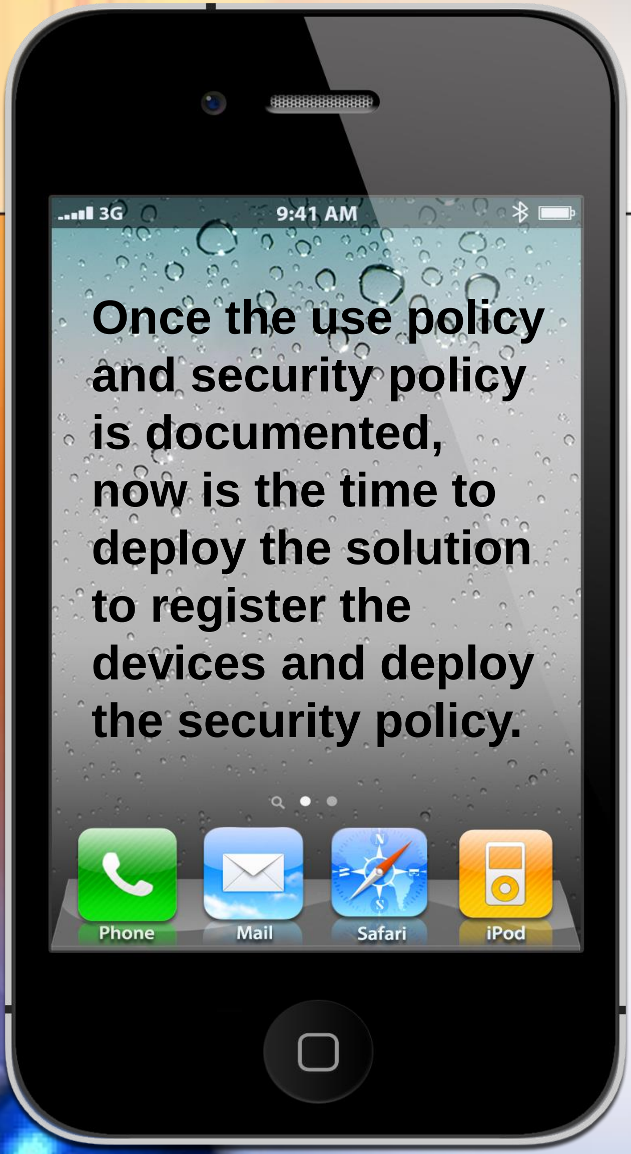
Step 3



Once the use policy is defined and the IT architecture designed, then the security policy needs to be documented to determine how the smart device will be secured to protect organization’s crown jewels.

- Step 3: Define the smart device security policy and security architecture. Consider the following:
  - Password Policy control
  - Encryption requirements
  - Port Control (WiFi, bluetooth, camera)
  - Remote lock/unlock/wipe
  - Asset tracking
  - Device configuration (VPN, Email, WiFi)
  - Delivery and control of applications to the device
  - Blacklisting/Whitelisting
  - Audit and Monitoring

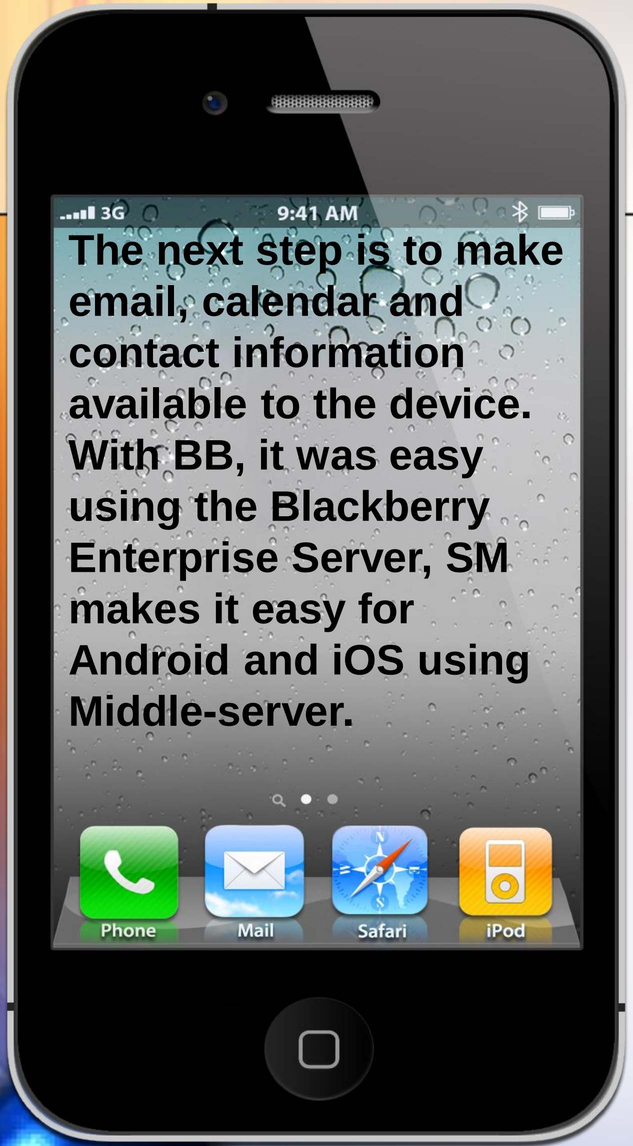
Step 4



Once the use policy and security policy is documented, now is the time to deploy the solution to register the devices and deploy the security policy.

- Step 4: Deploy the IT and security architecture and provision the device.
  - Provide emails of device owners to SM
  - SM sends a self-registry link to users
  - Users enter the registry information and obtain credentials
  - SM downloads the security policies on the device
  - Device is ready for use

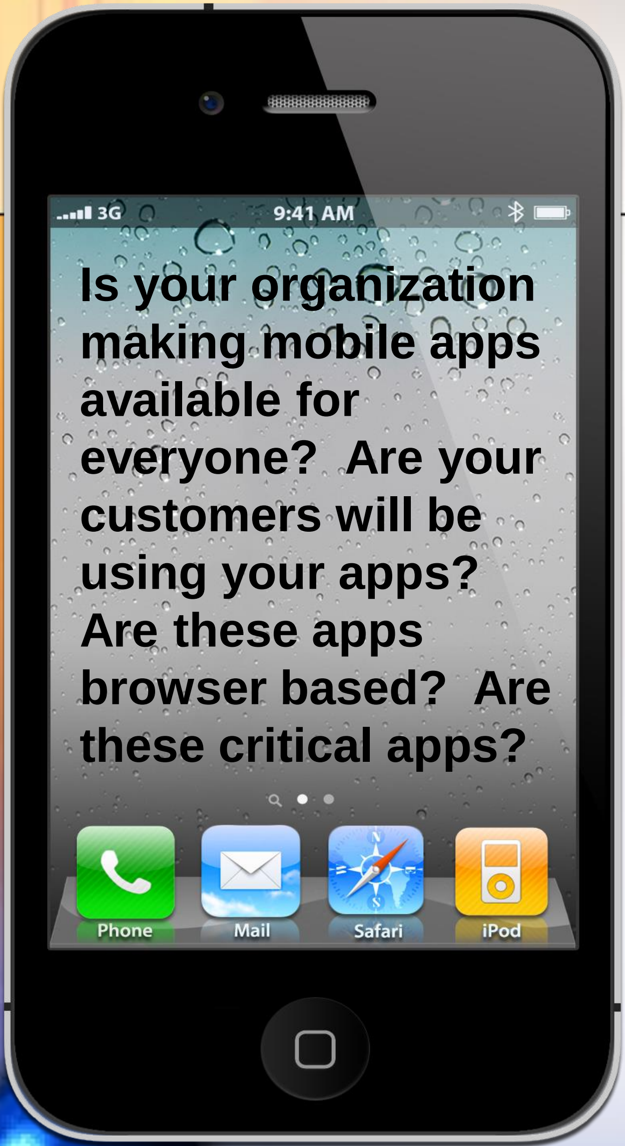
Step 5



The next step is to make email, calendar and contact information available to the device. With BB, it was easy using the Blackberry Enterprise Server, SM makes it easy for Android and iOS using Middle-server.

- Step 5: Enable Email, Calendar and Contact information on the device.
- For ActiveSync/Lotus Notes users
  - Combine ActiveSync/Lotus Notes capabilities with selected solution to implement email policies
  - Is the corporate anti-virus updated for mobile virus checks? Or should virus scan be performed by middle-server?

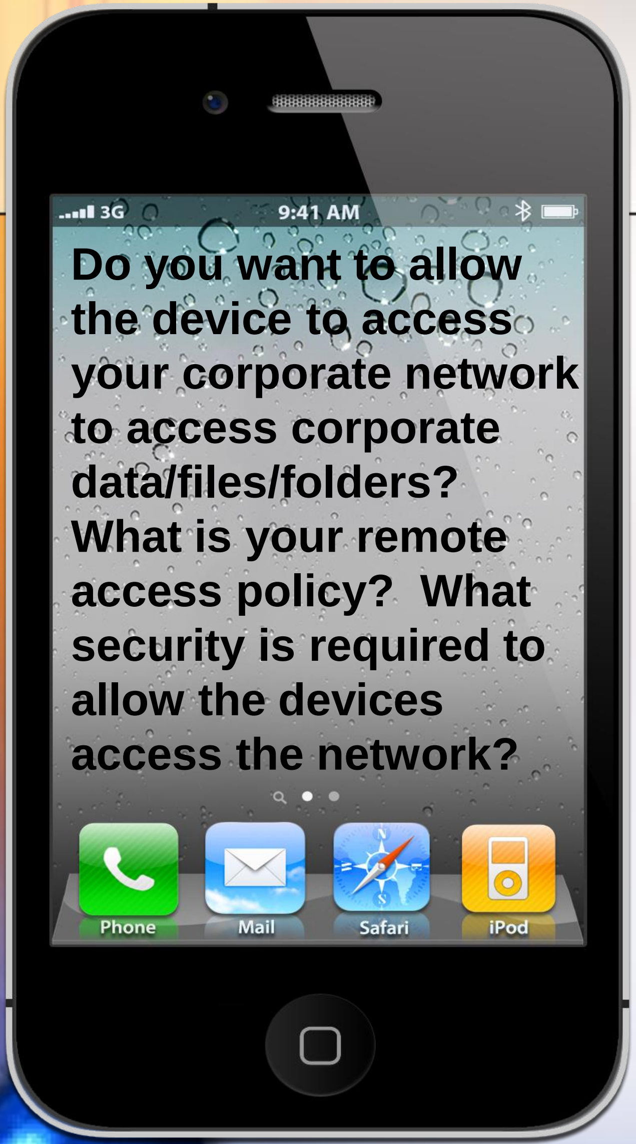
Step 6



Is your organization making mobile apps available for everyone? Are your customers will be using your apps? Are these apps browser based? Are these critical apps?

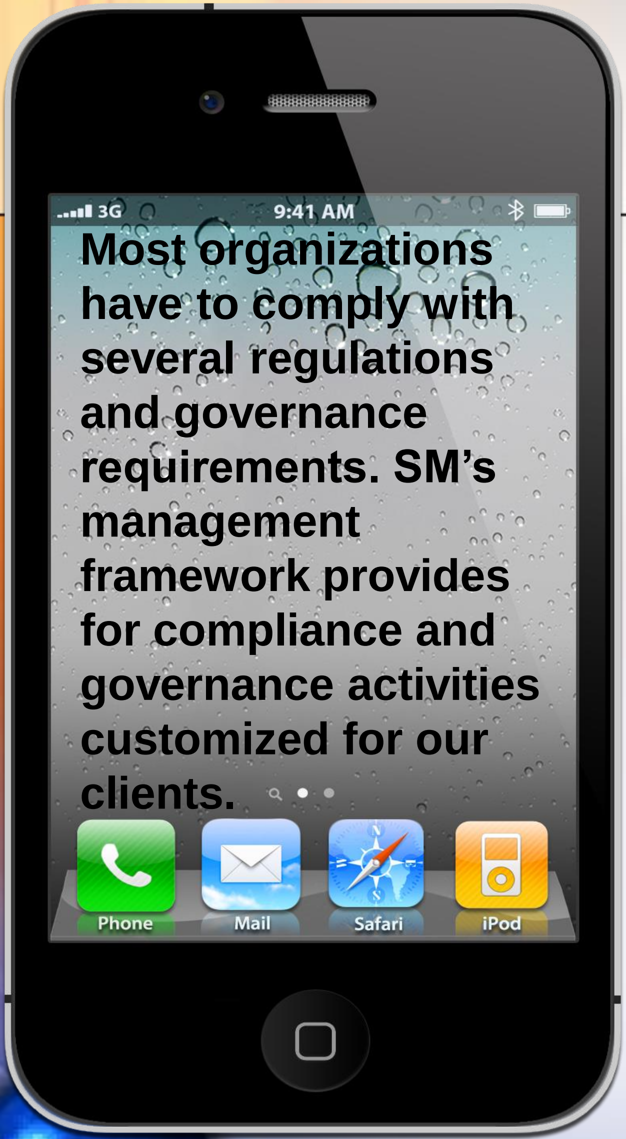
- Step 6: Enable deployment of corporate mobile applications on the device
  - Typically browser-based apps are enabled
  - Whitelisting/blacklisting policies are deployed?
  - Authentication protocols?

Step 7



Do you want to allow the device to access your corporate network to access corporate data/files/folders? What is your remote access policy? What security is required to allow the devices access the network?

- Step 7: Allow the device to access corporate network
  - – Remote Access Policy?
  - – VPN connection?
  - – Encryption policy?
  - – Authentication protocols?

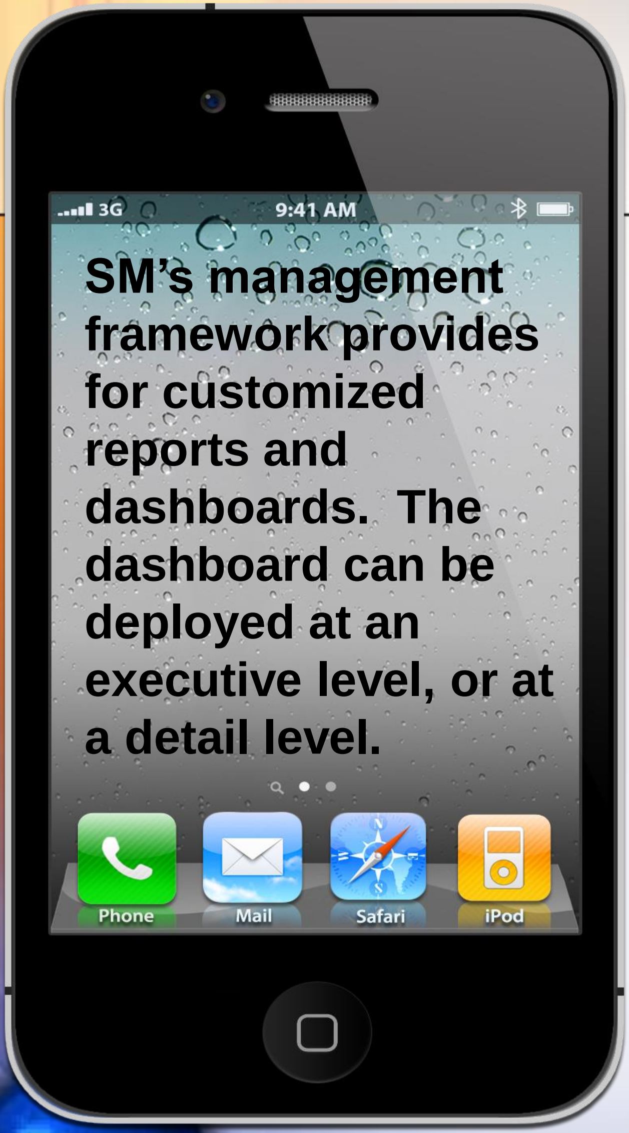


Most organizations have to comply with several regulations and governance requirements. SM’s management framework provides for compliance and governance activities customized for our clients.

Step 8

- Step 8: Manage regulatory compliance and governance requirements
  - – Health Insurance Portability and Accountability Act (HIPAA)
  - – Sarbanes-Oxley
  - – Payment Card Industry – Data Security Standard (PCI-DSS)
  - – IT Infrastructure Library (ITIL)

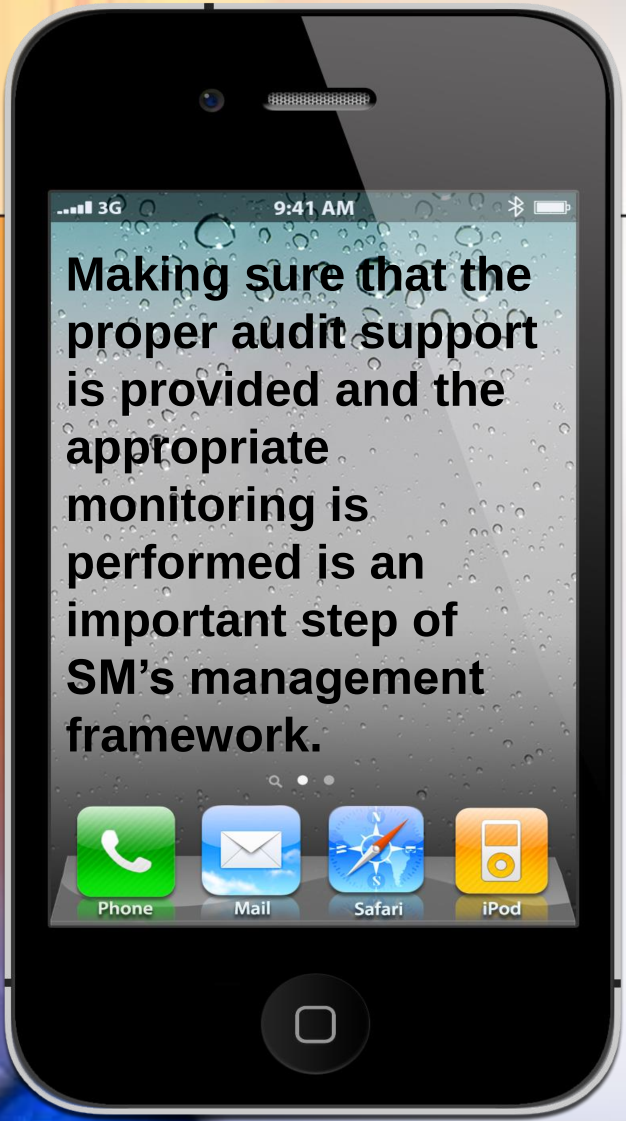
Step 9



SM's management framework provides for customized reports and dashboards. The dashboard can be deployed at an executive level, or at a detail level.

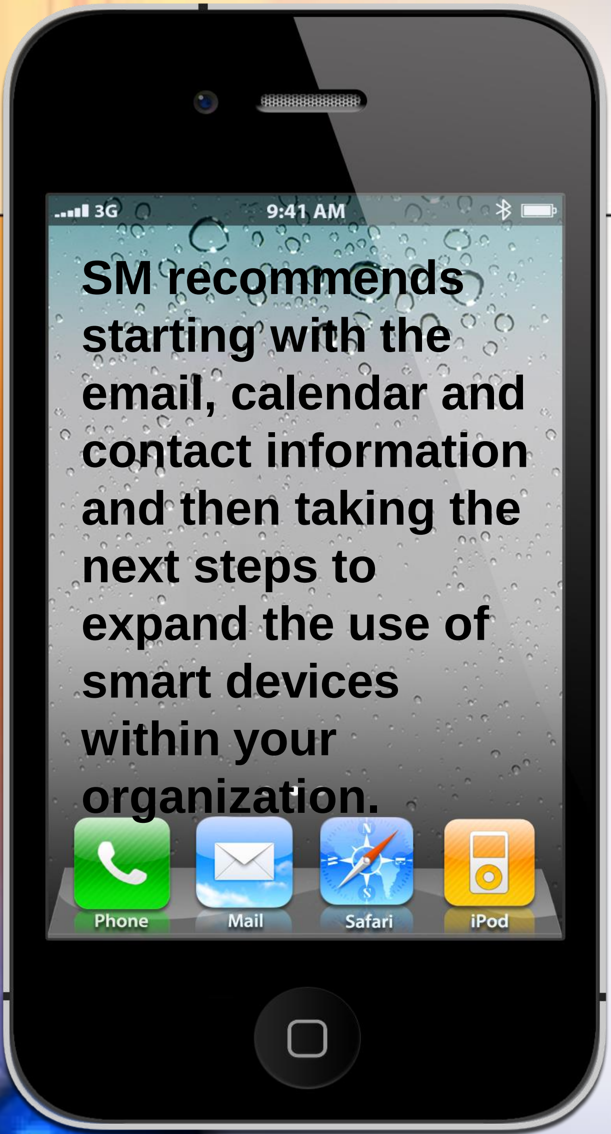
- Step 9: Manage reports and dashboard
  - – Executive and detailed dashboard
  - – Customize reports

Step 10



Making sure that the proper audit support is provided and the appropriate monitoring is performed is an important step of SM's management framework.

- Step 10: Manage monitoring and provide audit support
  - Real time vs. offline analysis
  - Audit support for smart devices



SM recommends starting with the email, calendar and contact information and then taking the next steps to expand the use of smart devices within your organization.

Case Study

An organization (BB users) wants to allow use of iPads and iPhones because most of the executives use these devices. Organization is a Microsoft Exchange user and wants to deploy custom browser based apps.

- Update/develop IT mobile use policy and mobile security policy
- Register non-BB devices to the SMS Server
- Push the security policies to the devices

Sajay Rai

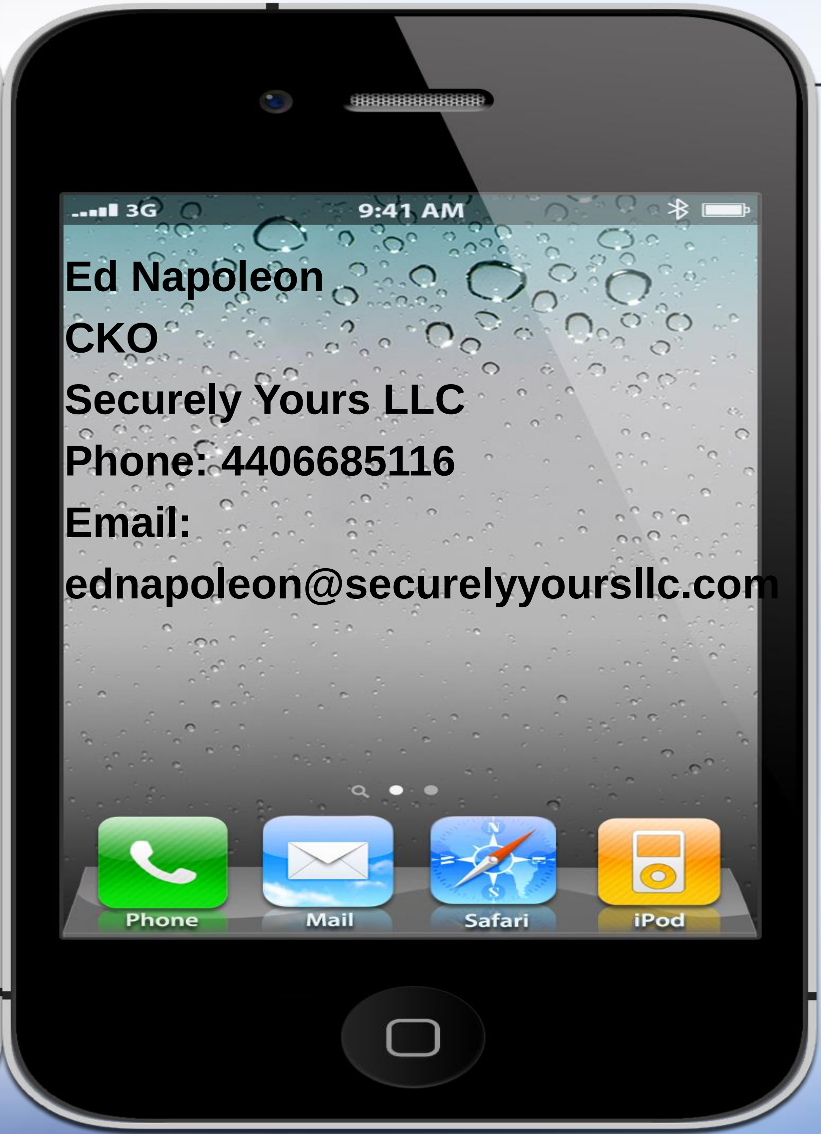
President and CEO

Securely Yours LLC

Phone: 216-288-4727

Email:

sajayrai@securelyyoursllc.com



Ed Napoleon

CKO

Securely Yours LLC

Phone: 4406685116

Email:

ednapoleon@securelyyoursllc.com

Security Features of iOS7

Feature 1

Single Sign-on

- Previously available for multiple apps developed by same developer (e.g. Google Apps)
- Now available for all Apps
- Some constraints:
  - Kerberos enabled platform and application
  - Still have to provision the device and send profile

Feature 2

Restricting opening of attachments

- Restrict attachments to open within approved apps (e.g. you can open an attachment in corporate email vs. personal email)
- Restricts data leakage
- Prevents users to take a picture of confidential information and post it on facebook

Feature 3

Default Data Protection

- When a passcode is configured, Apple used to protect the data using hardware encryption, but it was left for developers to protect application data (choice of encryption)
- Now, by default everything is encrypted

Feature 4

Per App VPN

- Instead of a VPN for the IP address, now the VPN is per App.
- Different Apps can connect to different VPNs
- Not fully tested yet, but I think we would be able to VPN to a payroll provider for payroll app and a bank for a banking application and both apps could be used interchangeably

Feature 5

Activation Lock

- Currently, the Find My iPhone feature allows you to locate and secure your lost iOS device using the Find My iPhone app on another iPhone, iPad or iPod touch, or by visiting iCloud.com on your computer.
- Unfortunately, it has a major drawback. The thief can turn off your iOS device and restore it to prevent you from using the Find My iPhone features.
- iOS 7 includes a new feature called Activation Lock. In iOS 7, turning off Find My iPhone or erasing your device requires Apple ID and password. It will also continue to display the custom message displaying your contact number, even after your device is erased. This should make it a major deterrent for thieves and make the Find My iPhone feature fool proof.

Feature 6

iCloud Key Chain

- In iOS 7, Safari's AutoFill feature has been extended to remember account names, passwords, and credit card numbers. Safari will automatically enter them when you visit a site to sign in or shop online. The keychain will also be synced via iCloud to all your iOS devices running iOS 7 and Macs running OS X Mavericks. Apple says the information will be stored using 256-bit AES encryption.
- Safari will also be able to generate a unique, hard-to-guess password like password management apps like 1Password.
- Unfortunately, this feature will be extremely useful only for users who use Safari on their computers and iOS devices. If you prefer using Chrome, then this feature is useless

Other Features

- Private Browsing
  - Easy to set private browsing on Safari
- Fingerprinting
  - Two factor Authentication
  - Still issues with it
    - Hackers
    - Ease of use
- Recent news of SIRI bug unlocking the phone

Use of Mobile Devices in DR

Enabling DR Responses via Smart Devices

BCP Definitions:

- **Business continuity planning** (BCP) "identifies an organization's exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, while maintaining competitive advantage and value system integrity”.[(Wikepedia)

- A business continuity action plan is a document that contains the critical information a business needs to stay running in spite of adverse events. (TechTarget)

Enabling DR Responses via Smart Devices

DR Definitions:

- Disaster recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. (Wikipedia)
- Disaster recovery is the area of security planning that deals with protecting an organization from the effects of significant negative events. (TechTarget)

Enabling DR Responses via Smart Devices

DR Issues Facing Organizations:

- How to efficiently and effectively notify the crisis management team when a disaster strikes?
- Where are the current disaster recovery plan documents?
- How do we monitor the progress of the recovery tasks when the crisis team is scattered around the world?
- How do we keep Business Continuity and Disaster Recovery plans current and updated?
- How do we make sure that the crisis team is aware of their responsibilities?
- How do we keep the crisis team contact information current?

Enabling DR Responses via Smart Devices

Key Elements of a DR Plan:

- **DR Policy**
- **Contact (Internal and External)**
- **Call Tree**
- **Functional Assessment (RTO and RPO)**
- **Monitoring**
- **DR Procedures**
- **Workflow**
- **DR Document Storage**
- **Tabletop Exercise and Test**
- **Training and Awareness**

Enabling DR Responses via Smart Devices

Communications as a Key Element of DR:

Majority of the items identified as key elements for DR, on the previous slide, require or are dependent on the Communications engine:

- Contact List
- Voice Communication
- Email Communication
- Text/Message Communication

Enabling DR Responses via Smart Devices

Communication is an essential part of DR:

- Must be timely
- Helps reduce Recovery Time Objective (RTO)
- Emphasized in BS25999-2
- Detailed in ISO 22301 (successor to BS25999)

Enabling DR Responses via Smart Devices

ISO 22301 requirements for Communications:

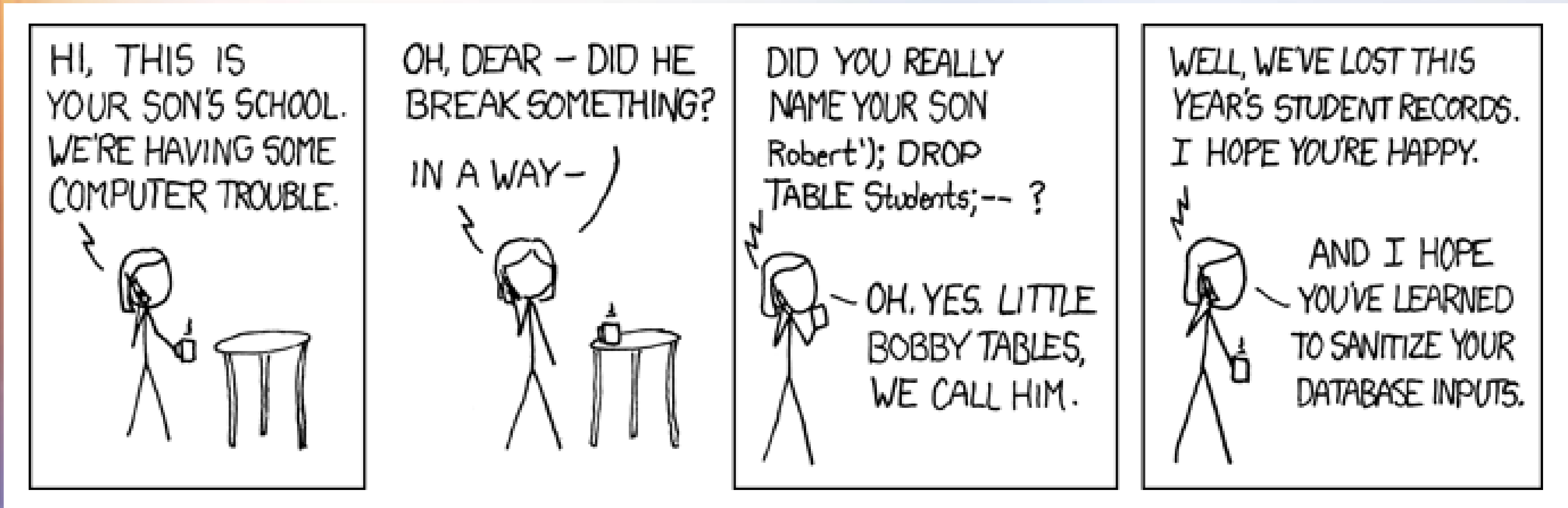
- Detect an incident
- Monitor incidents
- Internal communications within the organization
- Receive, document, and respond to national and regional risk advisory
- Assure the availability of communication media during an incident
- Facilitate communication with emergency incident responders
- Record incident information, decisions made, and actions taken

Enabling DR Responses via Smart Devices

Prerequisite for Enabling DR with Smart Devices:

- Issue a smart device to the Incident Response Team
- Configure the smart devices so that users cannot make changes to the smart device configuration settings, but can create and edit documents on the smart device
- A DR app may be needed for automation and workflow
- Do not be afraid to make mistakes, but learn from those mistakes and improve the DR process
- A mobile device manager (MDM) may be helpful

Enabling DR Responses via Smart Devices


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

xkcd.com

Enabling DR Responses via Smart Devices

How can you use Smart Devices to facilitate and improve DR response?

How do you enable the use of Smart Devices for DR?

Enabling DR Responses via Smart Devices

1. Load internal and external contacts into the smart device:

- Allows an organization to keep the contact information of the crisis management team, stakeholders, vendors, and government authorities current.
- Reminds the crisis team of their responsibilities in case of a disaster
- Allows the DR manager to perform a 1-Touch dial since the numbers are enabled

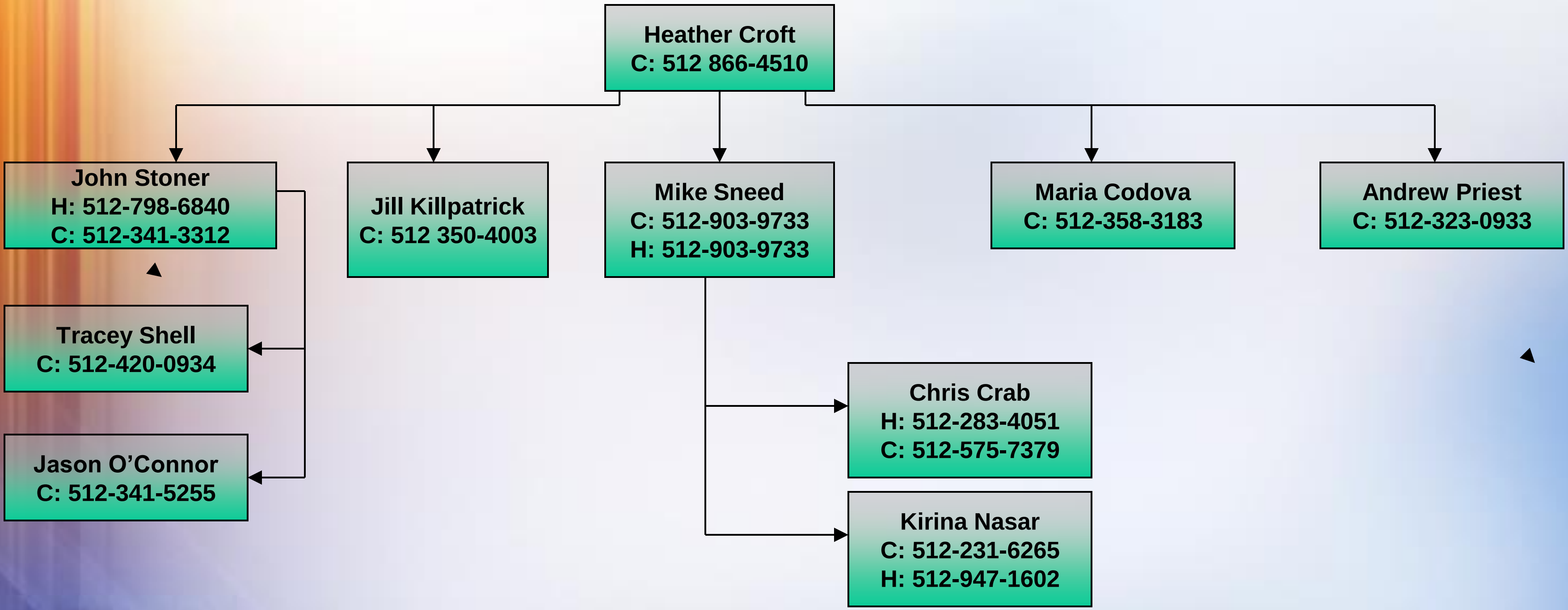
Enabling DR Responses via Smart Devices

2. Load the Call-Tree for incidents into the smart device:

- A Call Tree creates a calling structure that determines who to call first and who to escalate to when needed
- A DR app will possibly show the Call Tree as a graphics with enabled phone numbers
- Allows the DR manager to perform a 1-Touch dial since the numbers are enabled
- A real time chat capability which allows the crisis team members to communicate during recovery activities in a chat room

Enabling DR Responses via Smart Devices

Sample Call-Tree:



Heather Croft
C: 512 866-4510

John Stoner
H: 512-798-6840
C: 512-341-3312

Jill Killpatrick
C: 512 350-4003

Mike Sneed
C: 512-903-9733
H: 512-903-9733

Maria Codova
C: 512-358-3183

Andrew Priest
C: 512-323-0933

Tracey Shell
C: 512-420-0934

Jason O'Connor
C: 512-341-5255

Chris Crab
H: 512-283-4051
C: 512-575-7379

Kirina Nasar
C: 512-231-6265
H: 512-947-1602

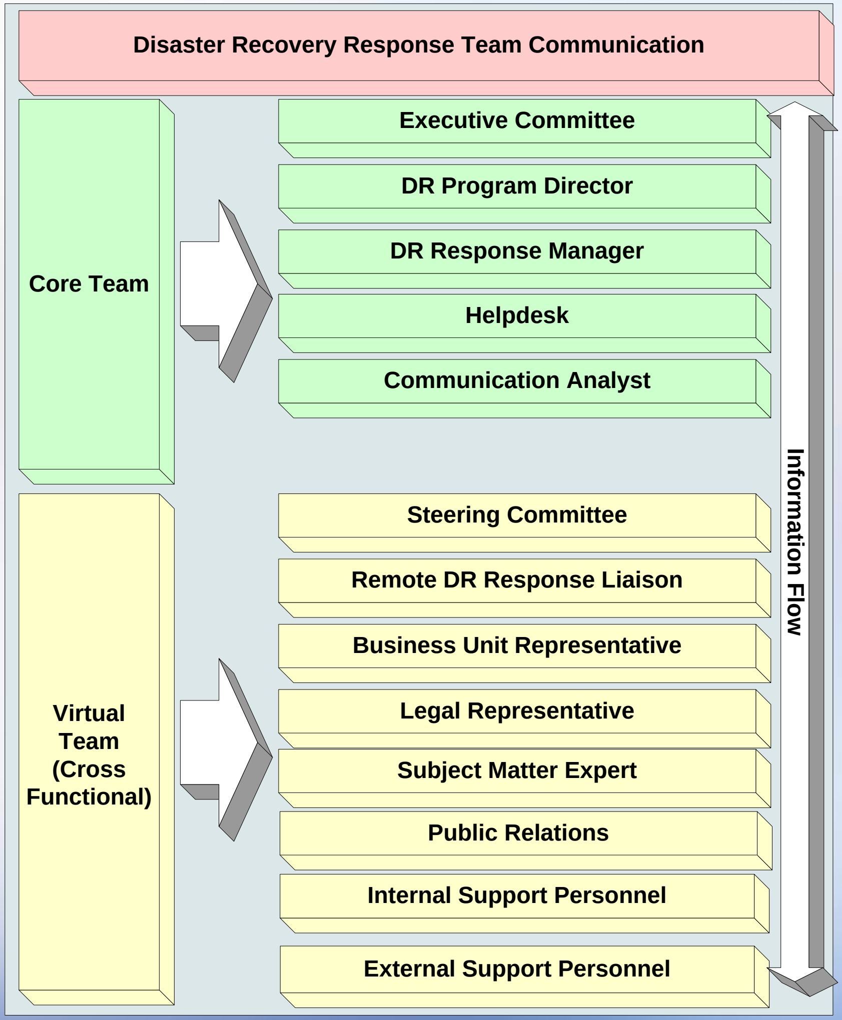
Enabling DR Responses via Smart Devices

3. Enable ISO 22301 based Communications:

- Allows internal communications between all levels and functions within the organization
- Provides the means for communications with external partners and stakeholders
- Provides for a means to send and receive documents and messages to stakeholders
- Assures the availability of means of communication during a DR incident

Enabling DR Responses via Smart Devices

Communication Teams



Disaster Recovery Response Team Communication

Core Team

- Executive Committee
- DR Program Director
- DR Response Manager
- Helpdesk
- Communication Analyst

Virtual Team (Cross Functional)

- Steering Committee
- Remote DR Response Liaison
- Business Unit Representative
- Legal Representative
- Subject Matter Expert
- Public Relations
- Internal Support Personnel
- External Support Personnel

Information Flow

Enabling DR Responses via Smart Devices

4. Incidence Response Logging:

- Allows recording of vital information about incident
- Allows recording of decisions made in response to incident
- Allows the recording of actions taken during response
- Logged information can include voice, video, chat, text, and documents
- Provides event tracking

Enabling DR Responses via Smart Devices

5. Load the Functional Assessment result (RTO and RPO) into the smart device:

- The goal of the assessment is to understand how critical any particular IT system is to the business operation, how quickly do business units want the system recovered (RTO), and how much data loss will the business tolerate in case of a disaster (RPO)

Application	Criticality: 1 – High 2 – Medium 3-Low	RTO: a-Always Available b- < 1 Hour c- < 24 Hours d- < 48 Hours e- 2-7 Days f- > 7 days	RPO: a-No Data Loss b- < 24 Hours c- 24 -36 Hours	Dependent on Business Cycle? 1 – Yes 2 - No
SAP	1	B	A	1
Database	1	B	B	1
Exchange Email	1	B	A	2
File System	1	C	C	1
Internet	2	D	N/A	2

Enabling DR Responses via Smart Devices

6. Monitor the DR process and procedures:

- Allows designated managers to review and update the recovery and response plans. It also allows the designated managers to activate the plan
- Allows DR and business managers to monitor progress
- Provides notifications to the crisis management team about the status of the recovery
- Allows the device to send periodic status notifications at the discretion of the DR manager
- Allows the designated managers to activate the plan

Enabling DR Responses via Smart Devices

7. Monitor the DR process and procedures:

- Notifies the DR team of an event
- Distributes the appropriate portion of the recovery/response plan to each team member
- May be used to provide correct execution time which can be used to update the RTO

Enabling DR Responses via Smart Devices

8. Store DR process and procedures:

- Allows DR team to load the recovery and response plans on the DR mobile server
- DR server can be hosted locally on your own server or offsite
  - Makes the DR process not dependent on the local network infrastructure
  - DR process becomes highly available
- DR team and business managers have access to DR procedures at all time during an incident
- Allows particular DR procedures to be pushed to the individuals responsible for the execution of the procedure on their smart device

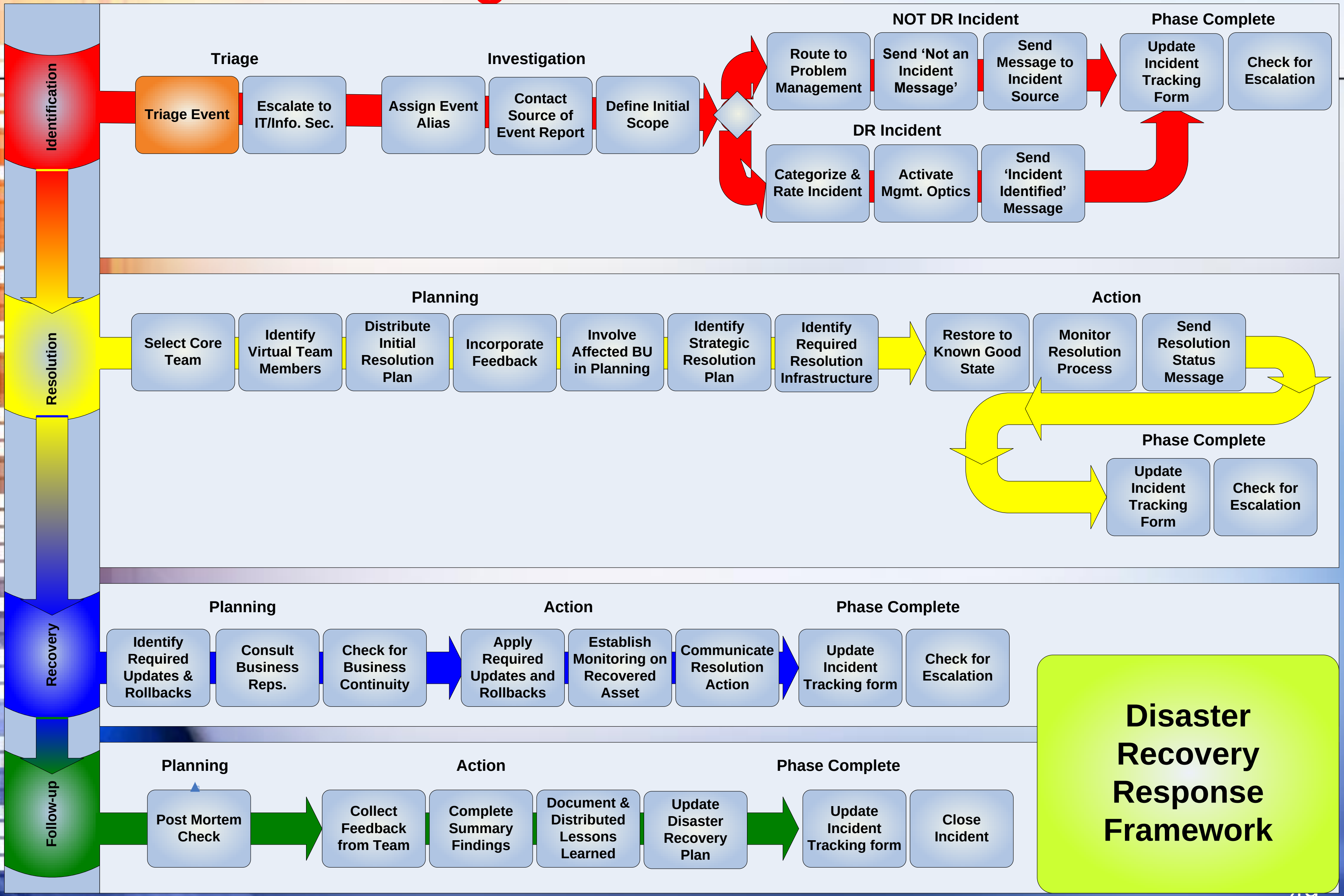
Enabling DR Responses via Smart Devices

9. Automate DR process and procedures:

- Allows IT to develop scripts and mobile apps that automate the DR process (explained in coming slides)
- Provides the automated monitoring and status reporting of the DR process
- Allows you to assign an owner (crisis management team member) to each task within every recovery and response plan loaded to the mobile DR server
- Provides a workflow based on the developed DR processes and procedures

Enabling DR Responses via Smart Devices

Automated High-level DR Process



Identification

Triage

Triage Event

Escalate to IT/Info. Sec.

Investigation

Assign Event Alias

Contact Source of Event Report

Define Initial Scope

NOT DR Incident

Route to Problem Management

Send 'Not an Incident Message'

Send Message to Incident Source

Phase Complete

Update Incident Tracking Form

Check for Escalation

DR Incident

Categorize & Rate Incident

Activate Mgmt. Optics

Send 'Incident Identified' Message

Resolution

Planning

Select Core Team

Identify Virtual Team Members

Distribute Initial Resolution Plan

Incorporate Feedback

Involve Affected BU in Planning

Identify Strategic Resolution Plan

Identify Required Resolution Infrastructure

Action

Restore to Known Good State

Monitor Resolution Process

Send Resolution Status Message

Phase Complete

Update Incident Tracking Form

Check for Escalation

Recovery

Planning

Identify Required Updates & Rollbacks

Consult Business Reps.

Check for Business Continuity

Action

Apply Required Updates and Rollbacks

Establish Monitoring on Recovered Asset

Communicate Resolution Action

Phase Complete

Update Incident Tracking form

Check for Escalation

Follow-up

Planning

Post Mortem Check

Action

Collect Feedback from Team

Complete Summary Findings

Document & Distributed Lessons Learned

Update Disaster Recovery Plan

Phase Complete

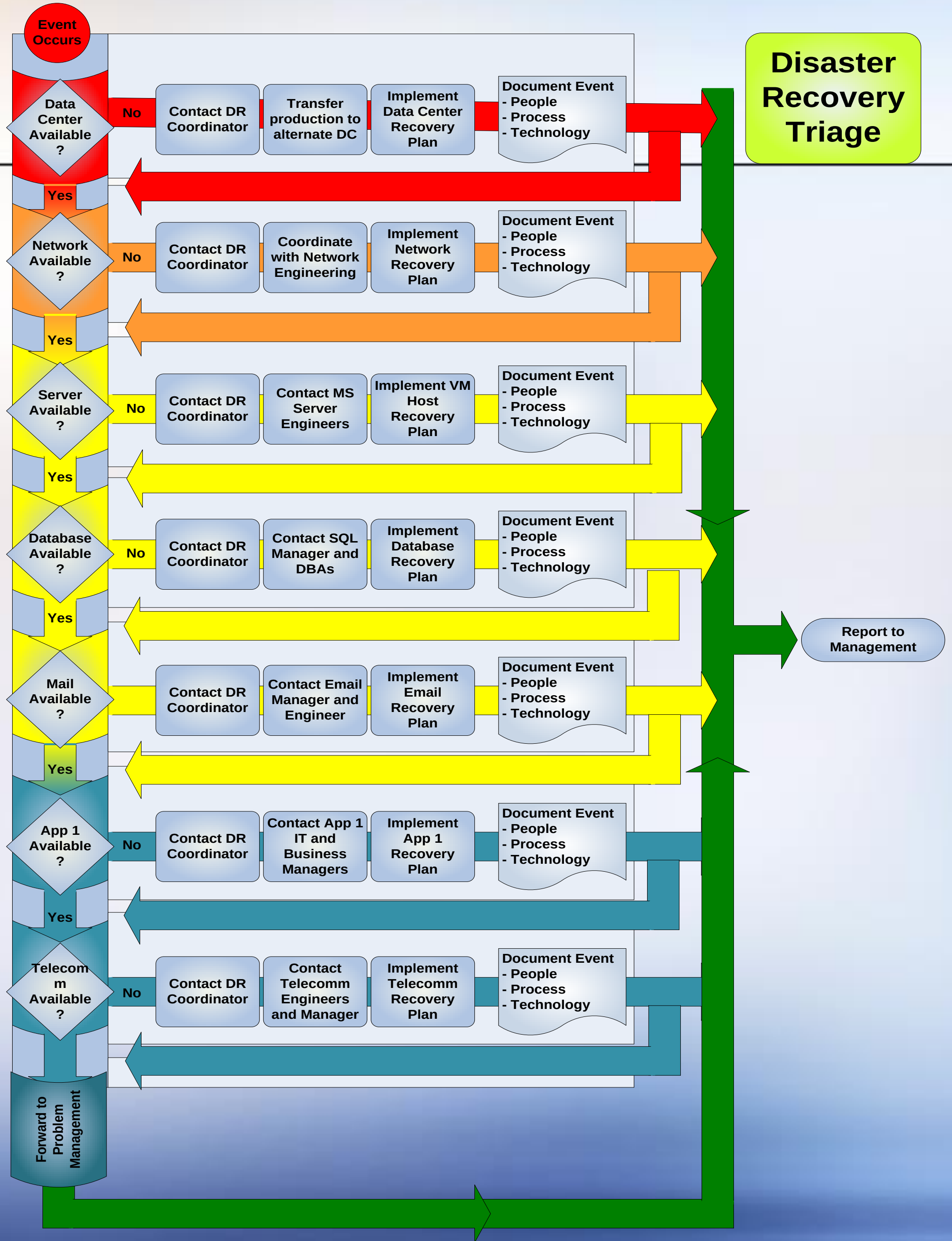
Update Incident Tracking form

Close Incident

Disaster Recovery Response Framework

Enabling DR Responses via Smart Devices

DR Triage



Event Occurs

Data Center Available ?
No
Contact DR Coordinator
Transfer production to alternate DC
Implement Data Center Recovery Plan
Document Event
- People
- Process
- Technology

Yes

Network Available ?
No
Contact DR Coordinator
Coordinate with Network Engineering
Implement Network Recovery Plan
Document Event
- People
- Process
- Technology

Yes

Server Available ?
No
Contact DR Coordinator
Contact MS Server Engineers
Implement VM Host Recovery Plan
Document Event
- People
- Process
- Technology

Yes

Database Available ?
No
Contact DR Coordinator
Contact SQL Manager and DBAs
Implement Database Recovery Plan
Document Event
- People
- Process
- Technology

Yes

Mail Available ?
Contact DR Coordinator
Contact Email Manager and Engineer
Implement Email Recovery Plan
Document Event
- People
- Process
- Technology

Yes

App 1 Available ?
No
Contact DR Coordinator
Contact App 1 IT and Business Managers
Implement App 1 Recovery Plan
Document Event
- People
- Process
- Technology

Yes

Telecomm Available ?
No
Contact DR Coordinator
Contact Telecomm Engineers and Manager
Implement Telecomm Recovery Plan
Document Event
- People
- Process
- Technology

Forward to Problem Management

Disaster Recovery Triage

Report to Management

Enabling DR Responses via Smart Devices

10. Tabletop Exercises:

- Allows DR manager to develop tabletop test script that can be loaded on smart devices
- Allows IT to perform DR tabletop tests and simulation on the smart device
- Makes it possible for participants in the test to be at various locations and still participate effectively
- Can provide simulation results and participants comments almost immediately after the exercise

Enabling DR Responses via Smart Devices

11. Provide DR Information to all Employees:

- Allows DR manager to publish assembly points
- Allows DR manager to push the primary and alternate DR locations to the primary incidence response team
- Allows DR manager to send text and email messages to the general employee base

Primary Disaster Location	
ADDRESS:	
PHONE NUMBER:	
FAX NUMBER:	
MAP LINK/GPS	
HOW TO FIND IT:	

Enabling DR Responses via Smart Devices

12. Training and Awareness:

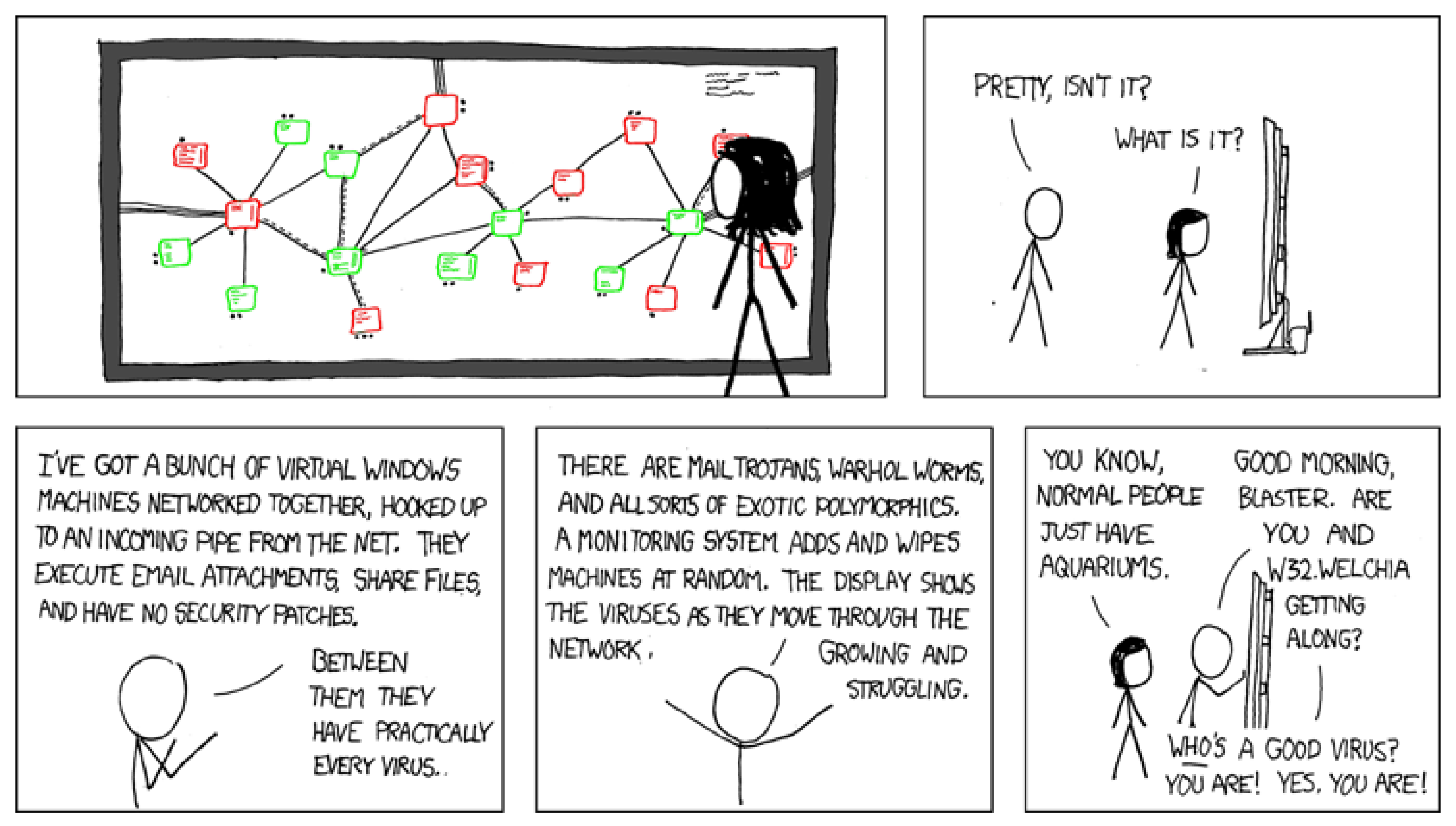
- Allows DR managers to develop and distribute DR training materials to the Incident Response Team (IRT)
- Makes it possible for participants in the test to be at various locations and still participate effectively
- Allows DR managers to collect all communications and discussions during a DR incident and use this information to update the DR plan and training material
- Allows for continuity of DR process should there be changes/turnover in resources

Enabling DR Responses via Smart Devices

13. Improving DR Response with Communication:

- Send timely and periodic messages to stakeholders using various channels
- Provide appropriate and sufficient content in the message
- Maintain control of the DR process, communication, and resources
  - Don’t Panic
- Be transparent

Enabling DR Responses via Smart Devices


PRETTY, ISN'T IT?
WHAT IS IT?
I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.
BETWEEN THEM THEY HAVE PRACTICALLY EVERY VIRUS.
THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK,
GROWING AND STRUGGLING.
YOU KNOW, NORMAL PEOPLE JUST HAVE AQUARIUMS.
GOOD MORNING, BLASTER. ARE YOU AND W32.WELCHIA GETTING ALONG?
WHO'S A GOOD VIRUS? YOU ARE! YES, YOU ARE!

Summary

Questions?