

RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

They Did What?!? – How Your End Users Are Putting You At Risk

SESSION ID: HT-F02

Mike Seifert

CISSP, CISA, CIPP, CISM, CGEIT
Vice President – Enterprise Risk & Resilience
Fiserv





New/future jobs



Cloud Services



Security Exceptions



Personal PC's



Instant Messaging



'Free' Stuff Online

admin Privileges



Cloud Storage



Personal Email



Tablets

User Temptations!



Porn



Peer to Peer



Printed materials



Clients and partners



Smartphones



Removable storage



Sharing via social media



Secrets and 'interesting' info

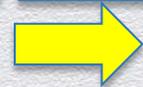


Wi-fi access points



User Risks

- ◆ Generally don't have simple technology solutions
- ◆ Incidents prompt us to ask "They Did What?!?"
- ◆ Are the results of user behaviors



Move this bar!

User Risks Are Not Often On Our Radar

Impact	Catastrophic	L	M	H	H	H
	High	L	M	M	H	H
	Medium	L	M	M	M	H
	Low	L	L	M	M	M
	Insignificant	L	L	L	L	L
		Rare	Unlikely	Possible	Likely	Certain
Likelihood						

We tend to focus Risk Management efforts on these events

These events are happening as we speak and are enabling larger ones

My Top 8

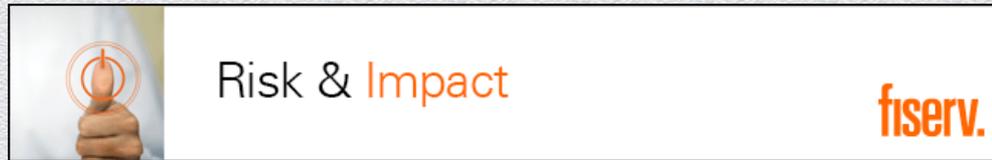
- ◆ Removed obvious risks. Focus on:
 - ◆ Overlooked
 - ◆ Oversimplified
 - ◆ Underestimated
 - ◆ Low Priority
 - ◆ Not anyone else's responsibility

Focus Areas

Phishing

Data Loss

Security Program



***1. Social Engineering
and Phishing:***

***Users may not identify external threats, or
exercise healthy skepticism, resulting in
compromised systems***

Cyber-Criminals are 'Knocking'

Legit LinkedIn Message

'Fake' – Phishing Email

Donna King has sent you a message

Donna King via LinkedIn to mikejseifert-yahoo.com via LinkedIn (7 hours ago)

LinkedIn

Donna King has sent you a message.
Date: 07/17/2012

You have 1 unread message from Donna King
<http://www.linkedin.com/nus-trk?trkact=viewMemberProfile&pk=member-h>

[View/reply to this message](#)

Don't want to receive e-mail notifications? [Adjust your message settings](#)

© 2012, LinkedIn Corporation

Test

Brendan Walsh via LinkedIn to Michael Seifert (2 minutes ago) [show details](#)

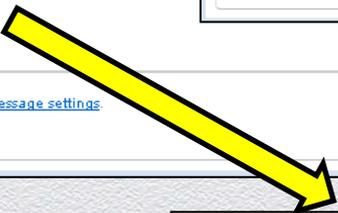
LinkedIn

Brendan Walsh has sent you a message.
Date: 7/17/2012
Subject: Test
This is a one line test message.

[View/reply to this message](#)

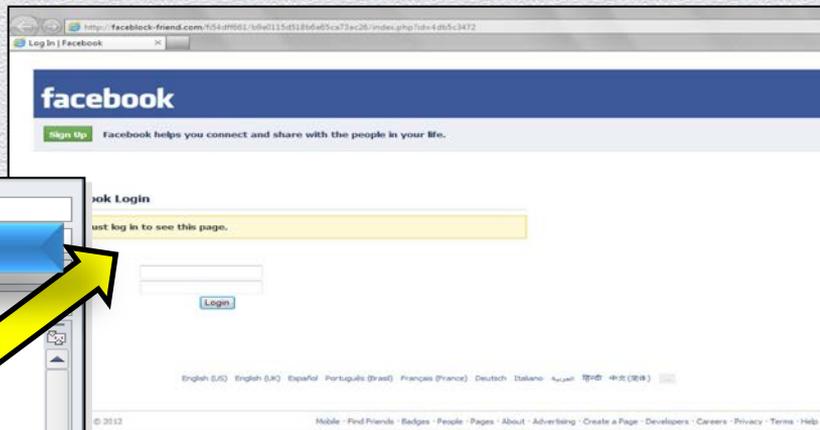
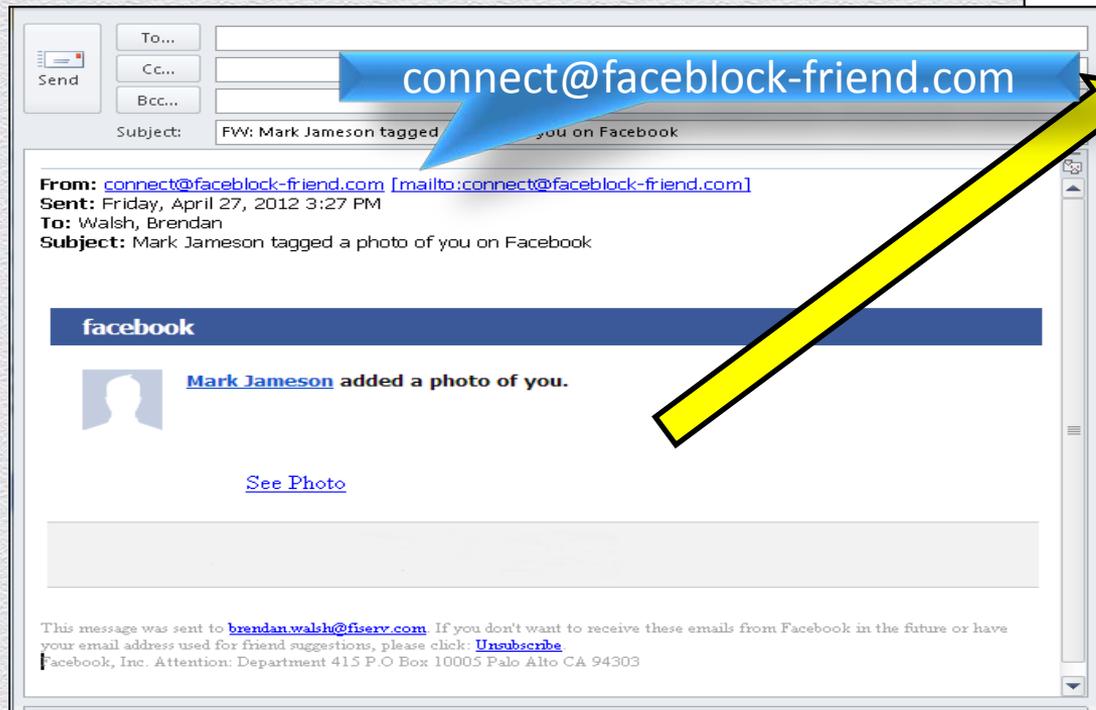
Don't want to receive e-mail notifications? [Adjust your message settings](#)

This email was intended for Michael Seifert. [Learn why we included this](#). © 2012, LinkedIn Corporation. 2029
Stierlin Ct. Mountain View, CA 94043, USA



<http://188.65.115.136/~chutne38/walcott.html>

Phishing - Facebook



- 18% clicked through to this fake site
- 8% entered their login credentials

Phishing – Mailbox Quota

From: IT Department [<mailto:itdept493@marketing38493.com>]
Sent: Friday, June 22, 2012 03:03 AM
To:
Subject: Mailbox Size Limit

itdept493@marketing38493.com

Attention Employee,

Your email mailbox is at or near it's size limit. If you would like to request a higher size limit, please access the link below and complete the request form.

[Click here to access now.](#)

If your login doesn't work resolve the issue.

Thanks,

Jim Garvens



“Yes, please increase my mailbox size. My manager is copied on this email thread. Thank you!!”

“Approved.” (reply from above’s manager)

- 11.4% Clicked through to fake website
- 7% Submitted form

Name:

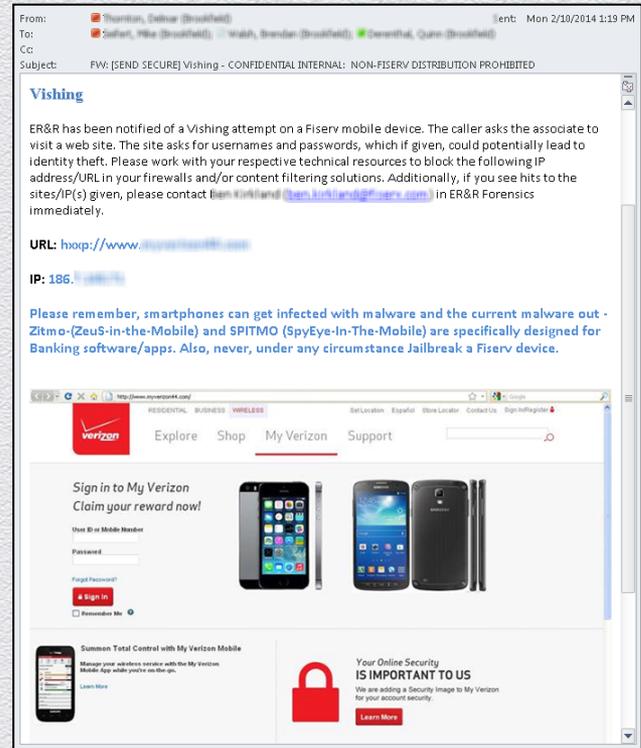
Email Address:

Business reason for increase

Submit

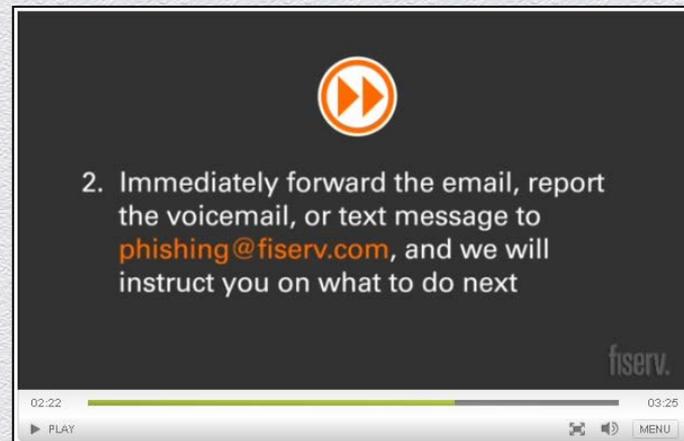
Effectiveness is Alarming and Evolving

- ◆ Technical defenses are futile!
- ◆ Per 2013 vendor testing stats in small/medium FI's, average response rates exceed 60 %:  **PhishLine.com**
Measured Security Awareness
 - ◆ Employee surveys
 - ◆ Mailbox quota exceeded
 - ◆ Company social events (company picnic, motorcycle ride and runs)
- ◆ Risks are evolving (QR Codes, text messages, apps, and others)



1. Program and Control Considerations

- ◆ Incident response processes to block phishing and malware sites
- ◆ Standardize associate communications
- ◆ Digitally sign communications
- ◆ Content and SPAM filtering



1. Education and Associate Engagement

- ◆ Make it personal
- ◆ Does this message, in this context make sense?
- ◆ Try reactive approach
- ◆ Identify and report

You've been phished!

Fortunately, this was only a test by Fiserv and not a malicious attack.

Phishing is a deceptive and very simple method of performing a cyber attack. Phishing attempts are intended to trick you into doing something unsafe that usually results in divulging potentially sensitive information or infecting a computer or network.

Please note that identifying information about you is not reviewed as part of this test. This test is part of our continuing education on the very serious computing risks that we face each day. If this were a true phishing attempt, your actions could adversely impact both you and Fiserv.

For more information please see the following:

- Review the Phishing section of the Acceptable Use and Secure Computing Standards found on Mainstreet
- Review the Phishing Awareness page on Mainstreet.
 - >Enterprise Risk & Resilience - Home
 - >Enterprise Security and Control Standards
 - >Security Awareness Training
 - >Phishing Awareness
- Review the pointers below to better educate yourself on how you could have determined that this email was suspicious

If you have additional questions about this or phishing risks, please contact your business unit's Information Security Officer.

The screenshot shows an email from 'LinkedIn Help Center' with several red callouts pointing to suspicious elements:

- From: LinkedIn Help Center <support@linkedin-connect.com>
- Subject: LinkedIn Help Center
- Callout: "The sending email address is not using a legitimate domain, it is using linkedin-connect.com. Similar, but not quite right."
- Callout: "This header is just an image, the links do not work."
- Callout: "Add another email address to help your account current and accessible."
- Callout: "Hover over this link with your cursor and you will see that it directs you to the same domain as above, linkedin-connect.com, and not the legitimate linkedin.com domain."

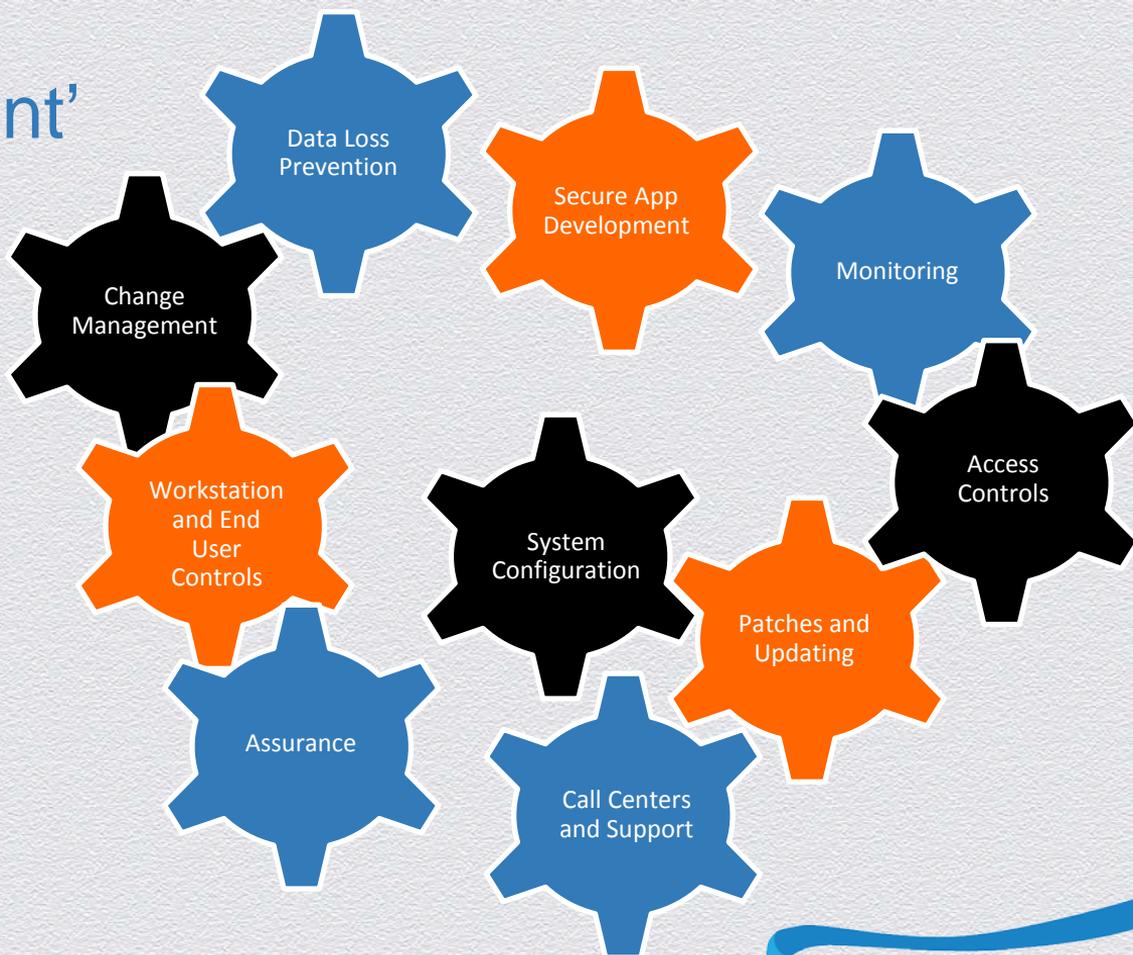
The email body contains a warning about suspicious activity on a LinkedIn account and provides instructions on how to secure the account, including adding a second email address.

2. Insiders

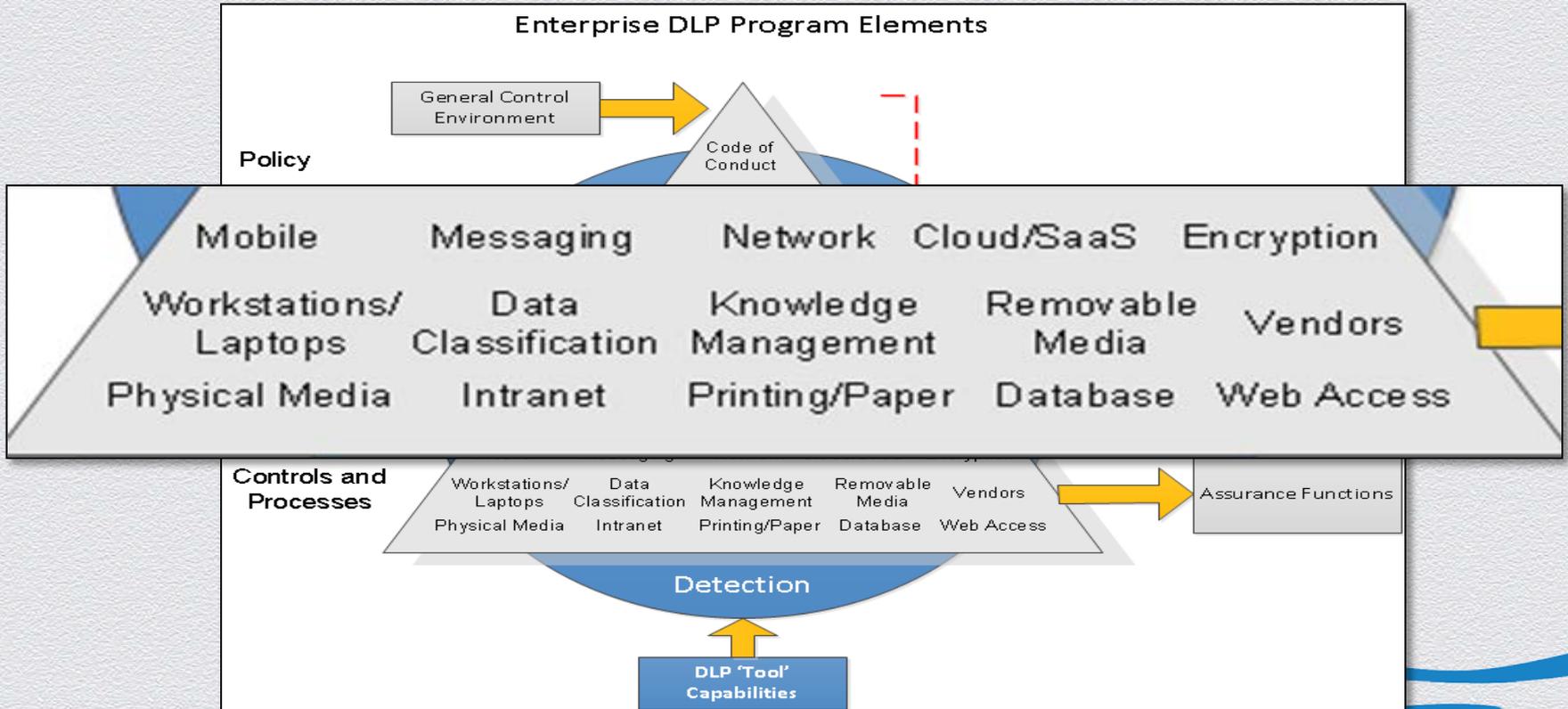
Knowledgeable insiders will attempt to circumvent or disable controls

A Control 'Environment'

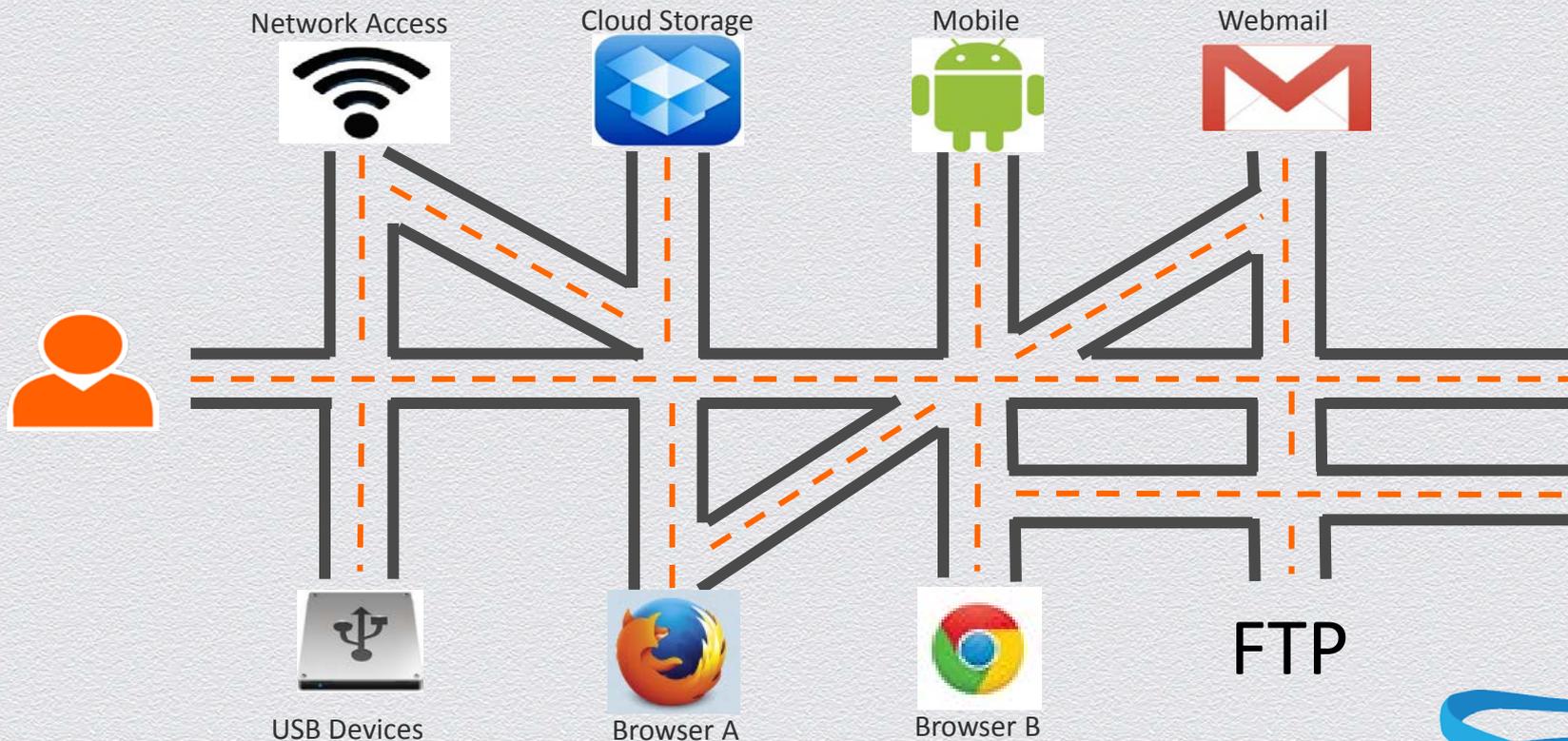
- Effective controls have dependencies and are 'complimentary'
- The 'Basics' are essential!
- 'Bad guys' look for opportunities



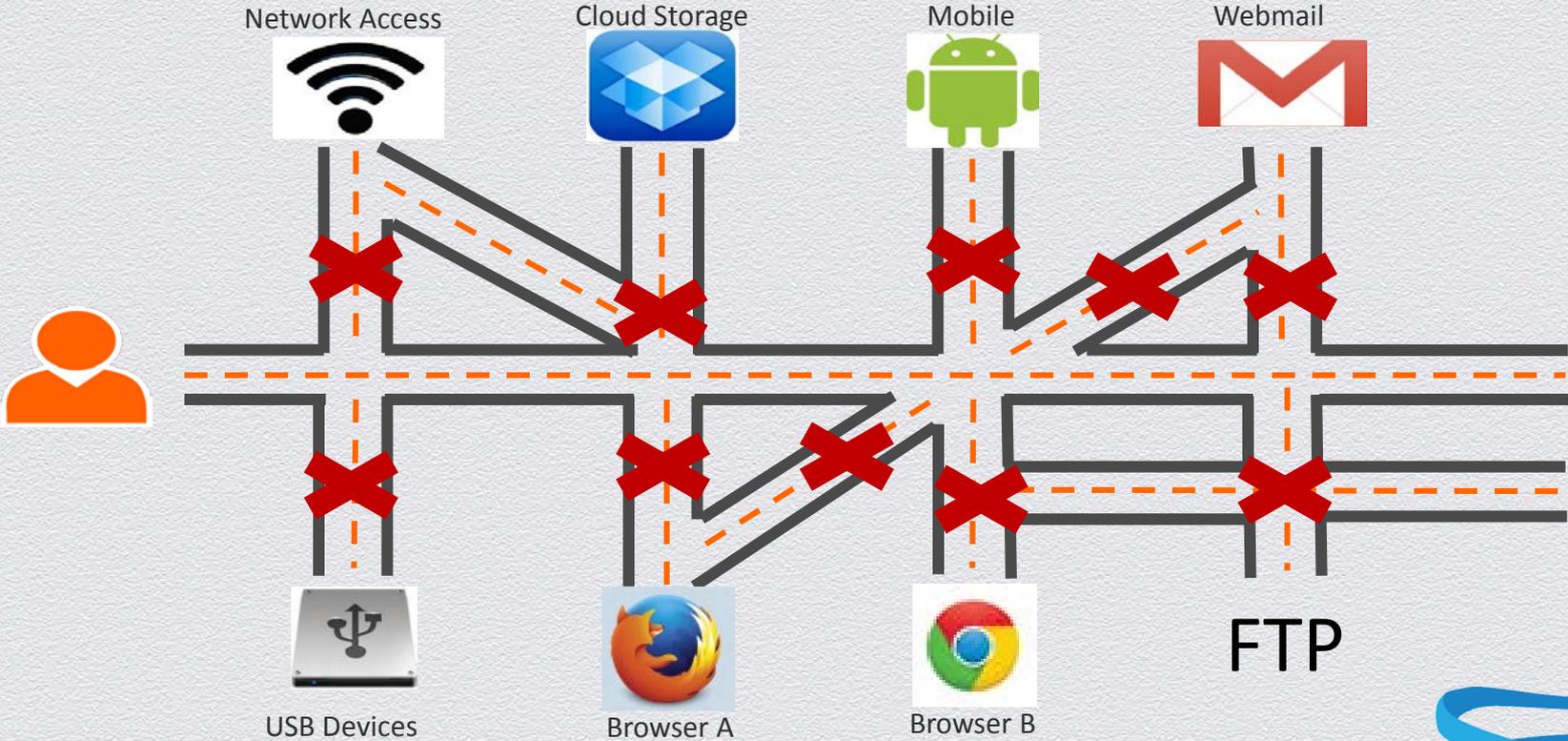
Data Loss Control Dependencies



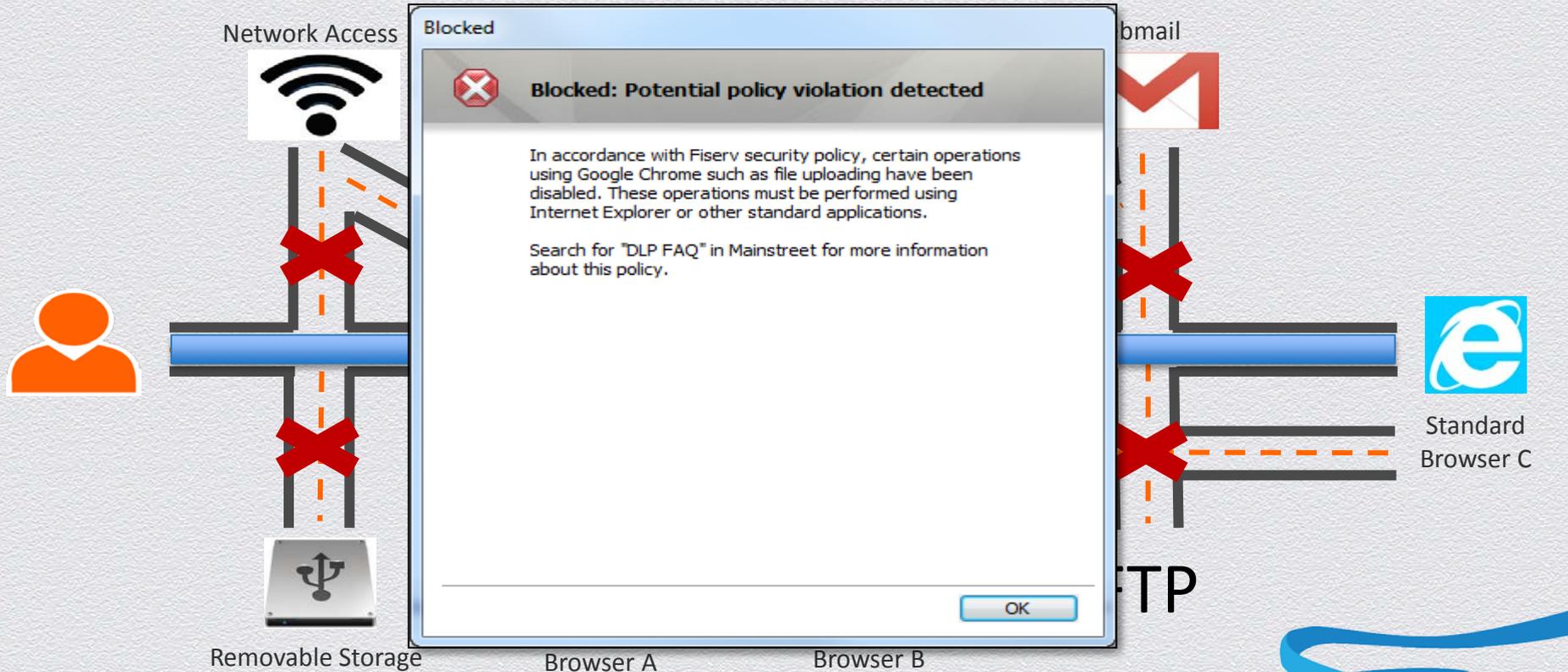
Understand Data Movement 'Channels'



Apply Controls

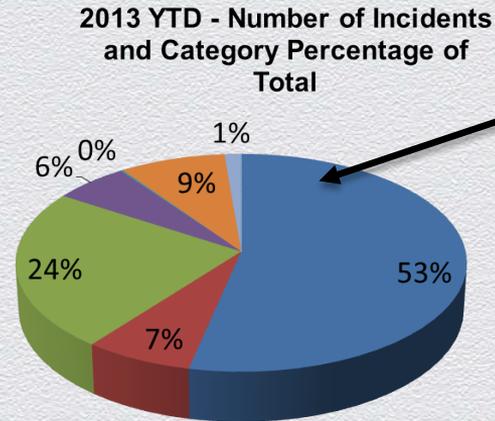


Standardize and Monitor



2. Program and Control Considerations

- ◆ Robust Data Loss Prevention
- ◆ Monitor controlled 'channels' for data movement, block or disable everything else
- ◆ Thorough and continuous gap assessments
- ◆ Personnel controls
- ◆ 'Layers'
- ◆ Workstation and device security configurations



Company docs
to personal
email accounts

2. Education and Associate Engagement



Preventing Data Loss 10 Habits to Protect Information

Preventing data loss is the responsibility of all associates. Learn 10 key habits for responsible computing and preventing information loss at Fiserv.

Visit: [Mainstreet > Enterprise Risk & Resilience Community > Risk & Impact > Preventing Data Loss](#)

Risk & Impact

fiserv.

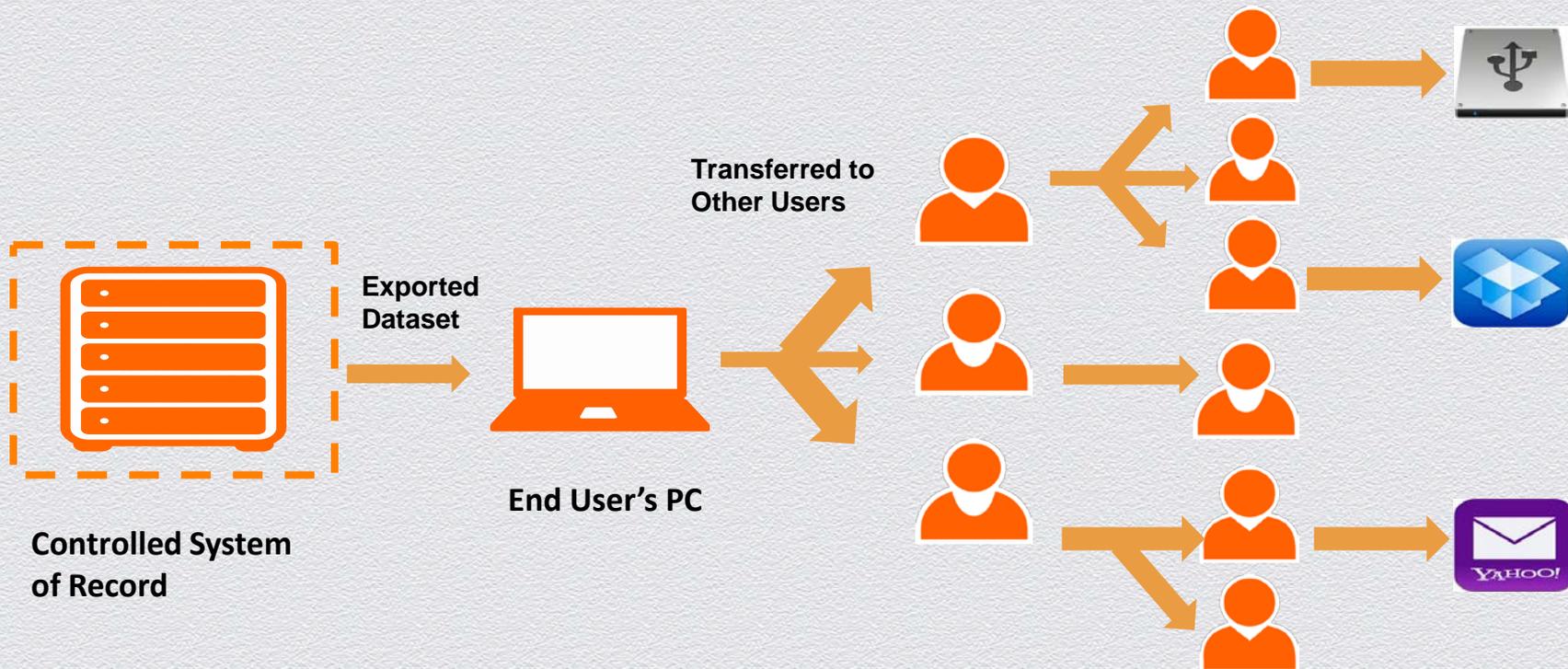
- ◆ Don't 'understate' your detection capabilities
- ◆ Closely guard monitoring capabilities and gaps
- ◆ Train security and technology associates on controls!!!
- ◆ Train users on approved 'channels'
- ◆ Equip users to educate third parties on requirements

fiserv.

3. Data Proliferation

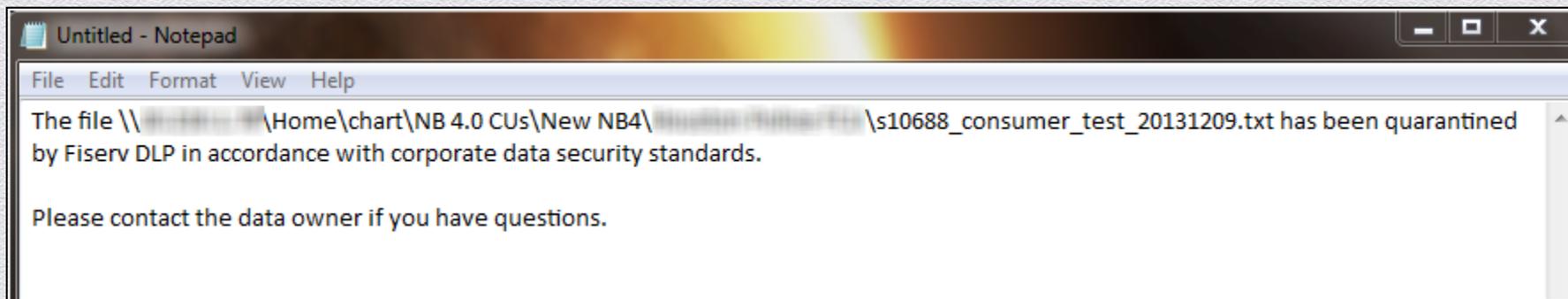
User actions and poor business processes contribute to the proliferation of company data (removing data from system of record)

How Is Information Really Handled?



3. Program and Control Considerations

- ◆ Keep information in its original, controlled system of record
- ◆ Restrict access for data exports
- ◆ DLP 'Discover' capabilities



3. Education and Associate Engagement



Stop Data Proliferation

Think before you copy.

Data proliferation occurs when information is copied, delivered, stored and recycled, sometimes over and over again. While modern technology makes this easy to do, this method of handling information makes it difficult for us to keep track of current versions and creates additional risks when the content includes sensitive information.

Use these quick tips to decrease data proliferation:

- Keep information in its system of record whenever possible.
- Think before copying, sending or forwarding information.
- Before sending any information, ask yourself:
 - How much is really needed?
 - Do the people I'm sending this to need all of this?
 - Would this person normally be authorized to access this?

Visit the Risk & Impact Series in the Enterprise Risk & Resilience Community on Manstreet to watch a video by Mike Seifert, Vice President of Risk Standards and Practices, to get more tips on how you can help control information and eliminate data proliferation.

Visit: [Manstreet](#) > Enterprise Risk & Resilience Community > Risk & Impact

Risk & Impact

fiserv.

- ◆ The best way to ‘secure’ data is to not have it in the first place
- ◆ Don’t create, don’t duplicate, destroy

4. Discretion

***Users do not properly identify sensitive data
or apply appropriate discretion in their
information handling practices***

Discretion Applies to All Actions

Transmission

Generation

Disclosure

Storage

4. Program and Control Considerations



Fiserv Data Classification and Labeling

In order to protect our confidential information, it must first be identified. All confidential information should be appropriately classified and labeled so others know how to handle it properly.

Visit the Risk & Impact section on the ER&R Mainstreet community to learn more about the data handling procedures and why correct usage protects our sensitive information.

Risk & Impact 

- ◆ Data classification and labeling system
- ◆ Monitor data movement systematically (DLP)
- ◆ Automated controls: labeling

4. Education and Associate Engagement

- ◆ Make issue personal
- ◆ Appropriate data usage, labeling, storage and handling
- ◆ Know and understand who you are disclosing information to

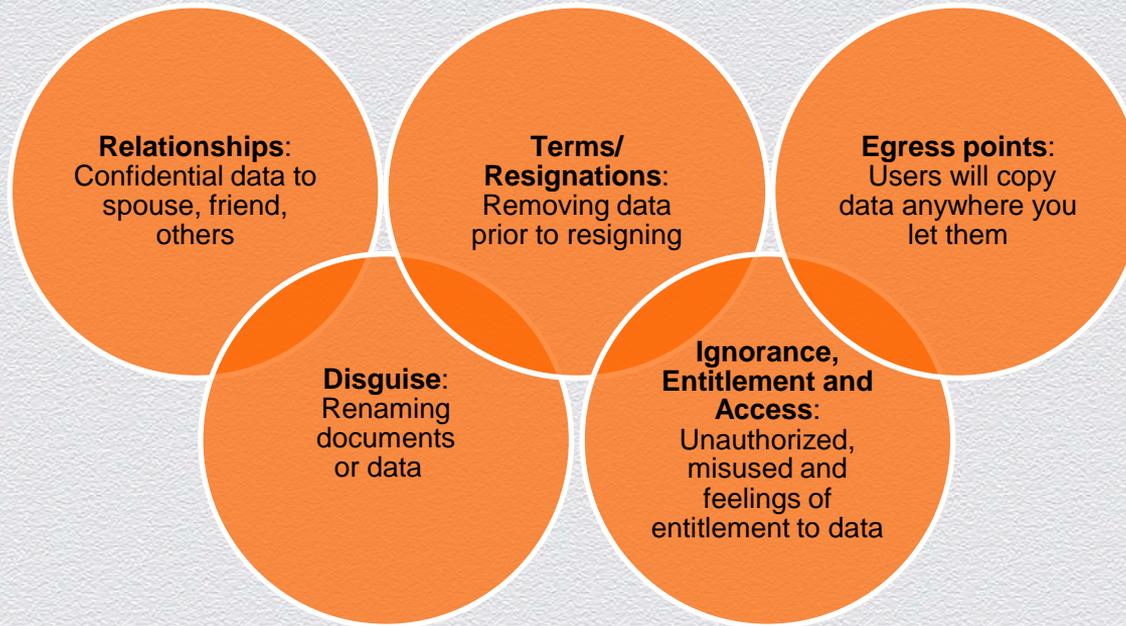


5. User Entitlement

Users feel entitled to any information/data they can access. If it can be accessed, it will be abused

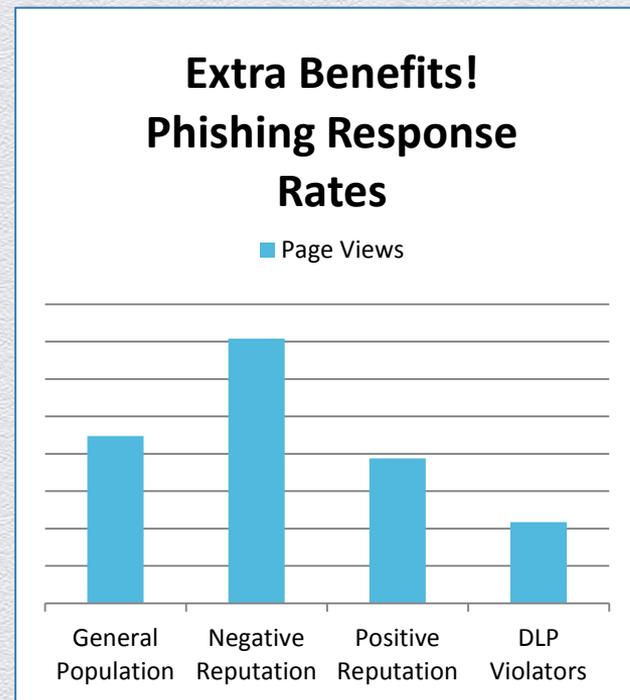
Data...at the mercy of your users

◆ Common DLP Incidents



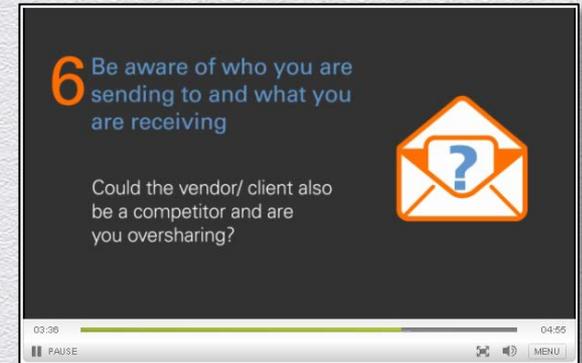
5. Program and Control Considerations

- ◆ Fast, effective incident response
- ◆ Effective access controls
- ◆ Data Loss Prevention and monitoring programs
- ◆ Digital Rights Management



5. Education and Associate Engagement

- ◆ Training on Acceptable Use Policy (security awareness)
- ◆ Monitor for, summarize and train on common risky behaviors



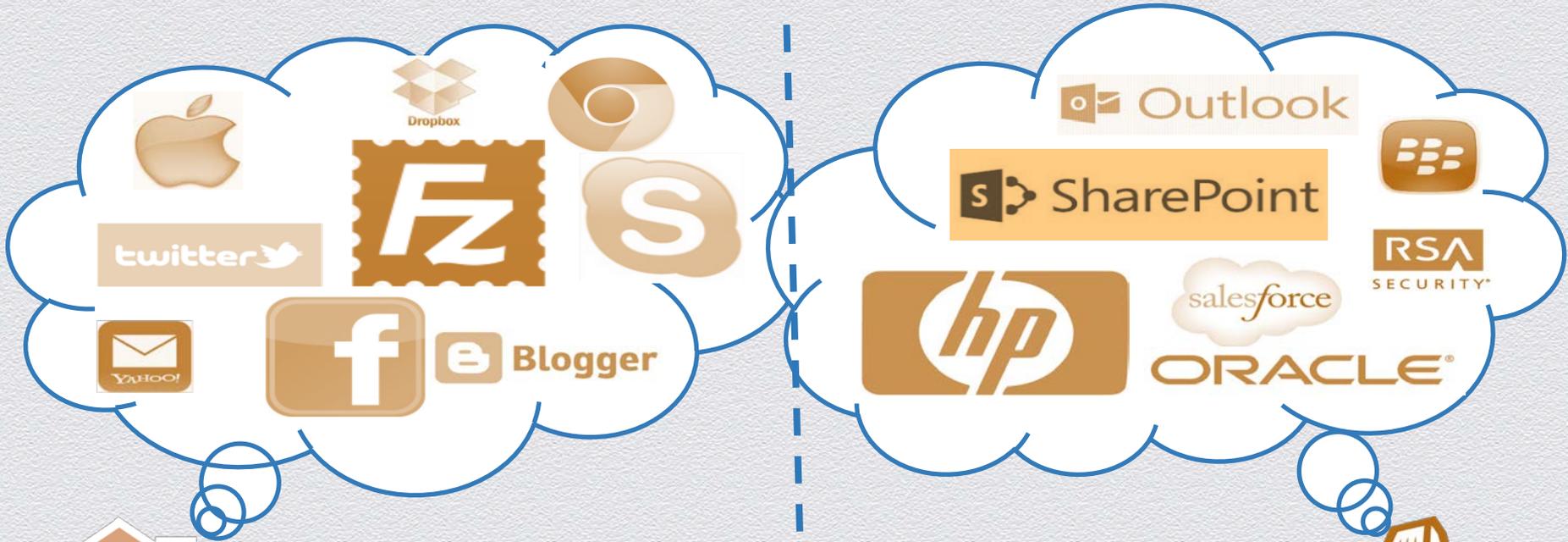
6. Separate Work and Personal

Users intermingle personal and work computing resources magnifying the impact of other risks

End User's Computing Universe



Go Old School



fiserv.



6. Program and Control Considerations

- ◆ Restrict corporate data to corporate assets
- ◆ ‘Containerize’ data on mobile devices
- ◆ Removable media controls
- ◆ Block or monitor cloud services and webmail



Fiserv Assets – Designed for Security

Fiserv assets include our approved computers, software, mobile devices, networks and email systems.

The use of approved assets to conduct company business establishes a necessary fence around our:

- Business information
- Trade secrets
- Confidential data

Only assets that have been approved by the company should be used when conducting Fiserv business. For more information on appropriate use of Fiserv assets, visit the Fiserv Risk & Impact Mainstreet community.

Risk & Impact 



6. Education and Associate Engagement



Know your ISO

Information Security Officers

Fiserv **Information Security Officers (ISO)** are your local experts on Fiserv security policies and standards, and how they apply to our business. The ISO plays a vital role in protecting our computing infrastructure, networks and information.

Get to know your ISO

Visit: [Mainstreet > Enterprise Risk & Resilience Community > Risk & Impact > Know your ISO](#)

Risk & Impact

fiserv.

- ◆ Segregate business and personal info
- ◆ Understand approved technologies and usage policies
- ◆ Know who to go to with questions

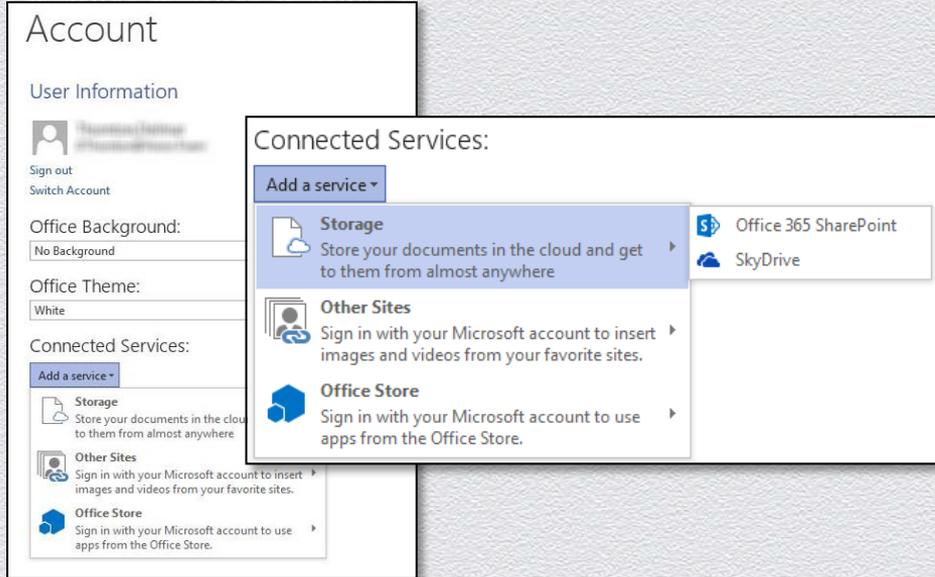
fiserv.

7. Millennialization

User consumer computing behavior and demands are driving business technology use-cases, preferred tools and product features

Convenience Prevails Over Control

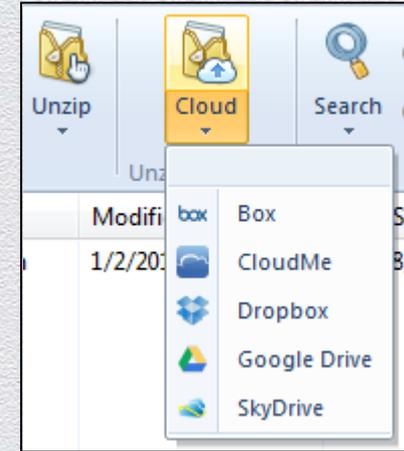
MS Office



iOS

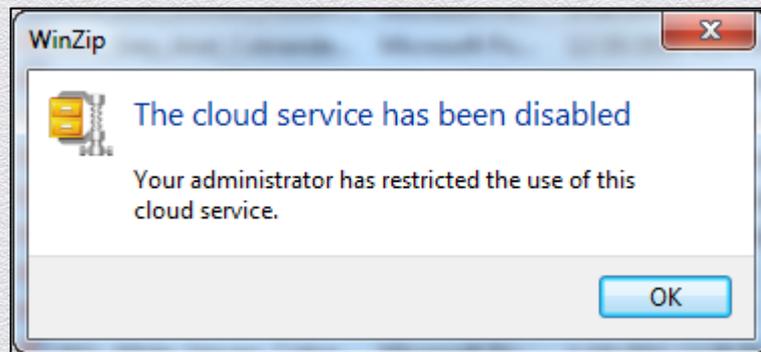


Winzip



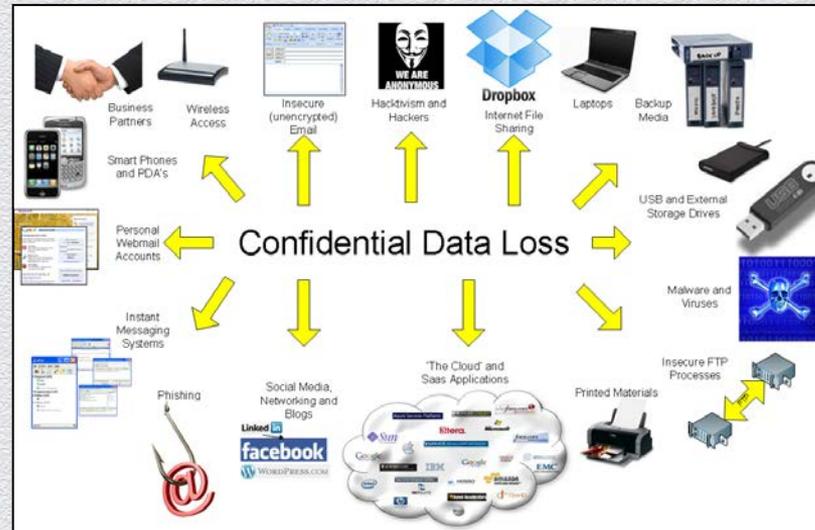
7. Program and Control Considerations

- ◆ Continually assess your environment
- ◆ Control workstations and mobile devices via policy
- ◆ Only permit assessed and approved software/services



7. Education and Associate Engagement

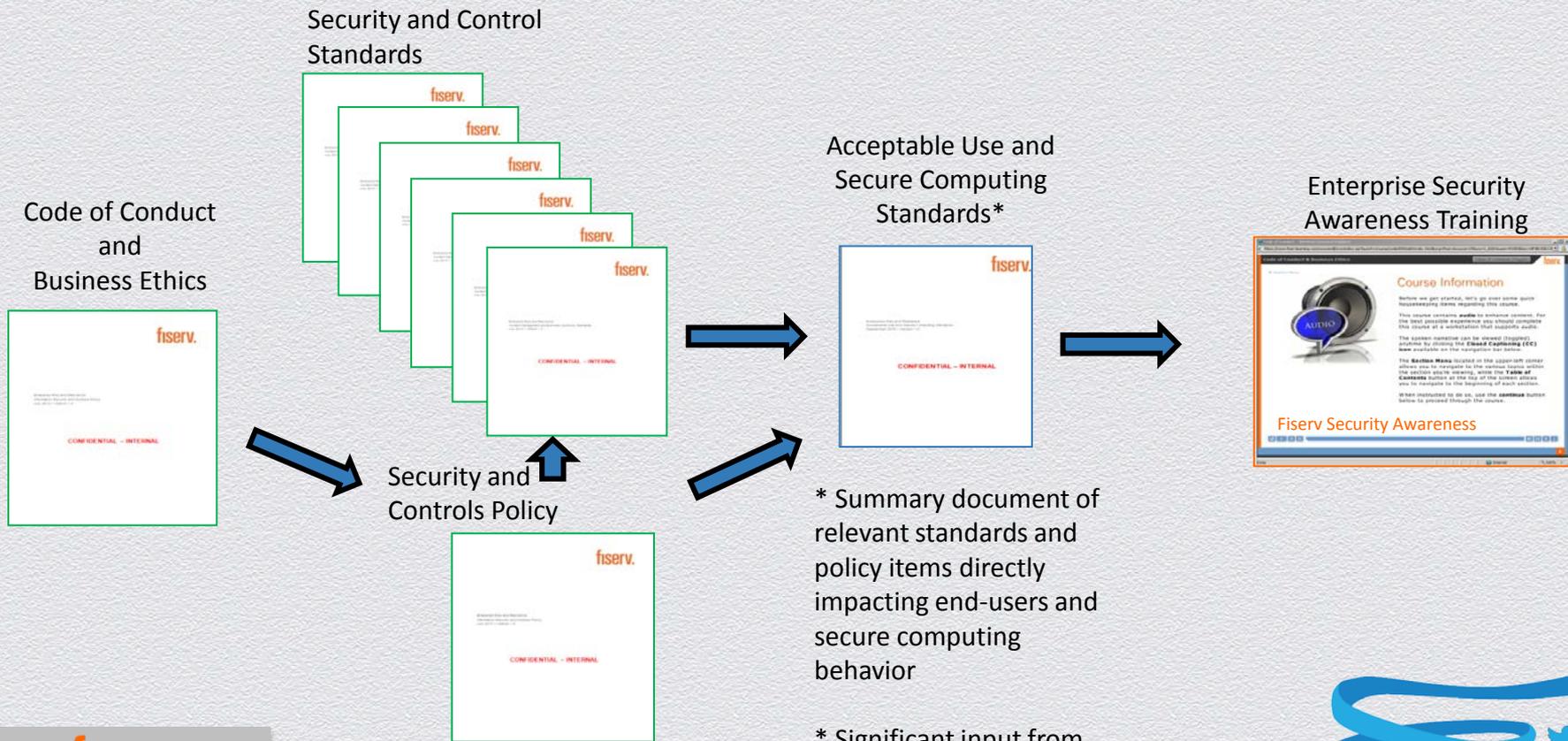
- ◆ Consult with security professionals prior to utilizing services
- ◆ Differences between work and personal information security imperatives



8. Enforce Standards

User ignorance, neglect or circumvention of security standards/policies will undermine strategy and comprehensive, layered security approaches

The Fiserv Model - Standards and Policies



* Summary document of relevant standards and policy items directly impacting end-users and secure computing behavior

* Significant input from Fiserv incident data

Exceptions and Accommodations



VS.



Productivity or Vanity?

8. Program and Control Considerations

- ◆ Enterprise standards program
- ◆ Require compliance and align with auditors, regulators, etc.
- ◆ Strong ‘Tone at the Top’
- ◆ Have consequences for non-compliance
- ◆ Robust, objectives-based exception process
 - ◆ Segregate environments if necessary



8. Education and Associate Engagement

- ◆ Understand and utilize your program
- ◆ Importance and benefits
- ◆ Negative event stories with a personal twist
- ◆ Leaders setting a positive example

Slide Title	Duration	Status
Welcome	02:12	
Welcome	00:11	
Before Beginn...	00:41	
What to Expect	00:20	
Training Over...	00:59	
What Is Security?	02:31	
What is Secur...	00:07	
Information S...	00:20	
Security Is No...	00:36	
Security Is Co...	00:26	
Security Is Dy...	00:48	
We Are Resp...	00:12	
Security Is Essent...	05:45	
Why is Securit...	00:09	
Security Is Im...	00:42	
Our Business ...	00:34	
External Thre...	00:55	
Data Is Const...	01:00	
Data Lifecycle	00:46	
Impact Of An ...	00:41	
Constant Introl...	00:36	
Risk	00:21	
Security is Essenti...	06:17	
How Does Fiserv ...	05:03	

Data is the Target

20 billion transactions every year

Exposure risks exist for information

- Transactions
- Movement
- Transfers
- Changes
- Access activities



Complex communication 'ecosystems'

- In Fiserv control
- Out of Fiserv control

© 2012 Fiserv, Inc. or its affiliates

FISERV CONFIDENTIAL - INTERNAL

07:57 / 34:43 Minutes

RSACONFERENCE2014

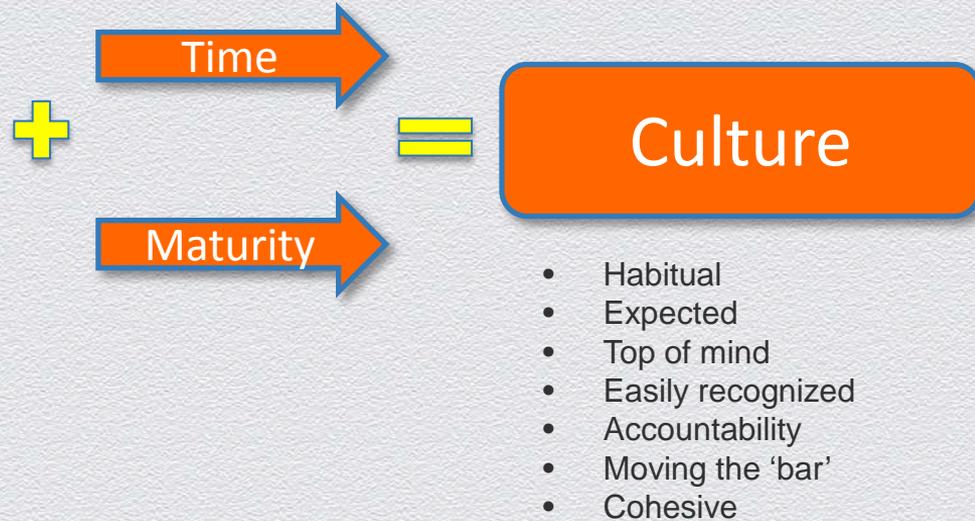
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Conclusion

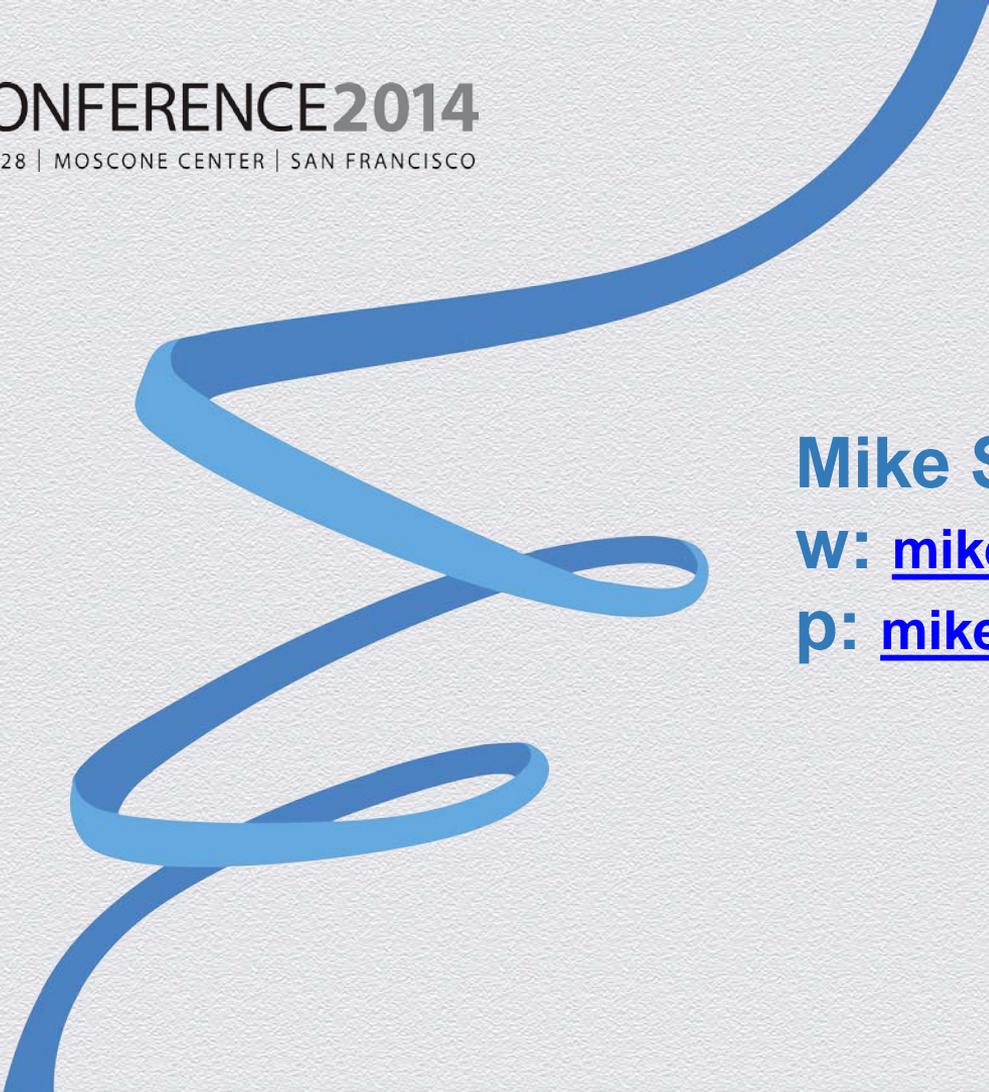
Conclusion – Essentials for Risk Management

1. Fast, effective incident response
2. Education – what, why and consequences
3. Understand controls, focus on objectives
4. Standardization
5. Never ‘assume’ anything



RSA[®] CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Mike Seifert

W: mike.seifert@fiserv.com

p: mike.seifert@nym.hush.com