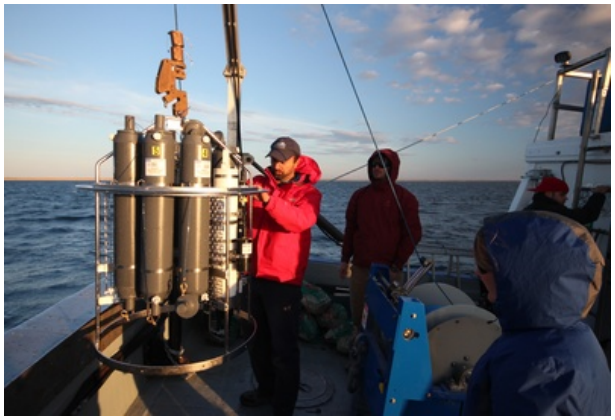
“Developing A Cyber Risk Strategy”

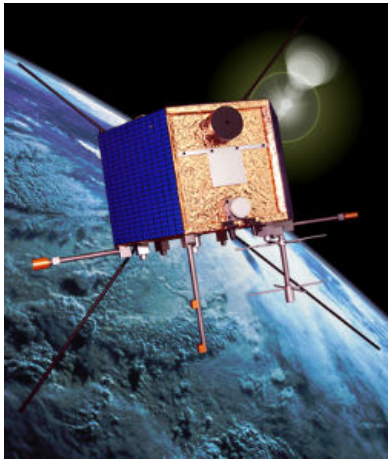
Janet Stein

RIMS Board Director
(The Risk and Insurance Management Society, Inc.)

March 2016

Janet Stein
Director Risk Management & Insurance, University of Calgary
RIMS Board of Directors





THE COST OF CYBERCRIME

Allianz estimated the annual cost of cybercrime for the world's top 10 leading economies, which account for more than half of worldwide losses.

United States
$108 billion

China
$60 billion

Germany
$59 billion

Brazil
$7.7 billion

United Kingdom
$4.3 billion

India
$4 billion

France
$3 billion

Russia
$2 billion

Japan
$980 million

Italy
$900 million

Source: Allianz Global Corporate & Specialty, *A Guide to Cyber Risk*

RIMS
the risk management society™

THE TARGET EFFECT

Level of Concern about Data Breach
(on a 10-point scale)

Before Target	5.7
After Target	7.8

Top 5 Changes Made to Operations and Compliance After Target

Created incident response team	56%
Conducted training and awareness activities	50%
Implemented data security effectiveness metrics	48%
Implemented new policies and procedures	48%
Provided specialized education for IT security staff	47%

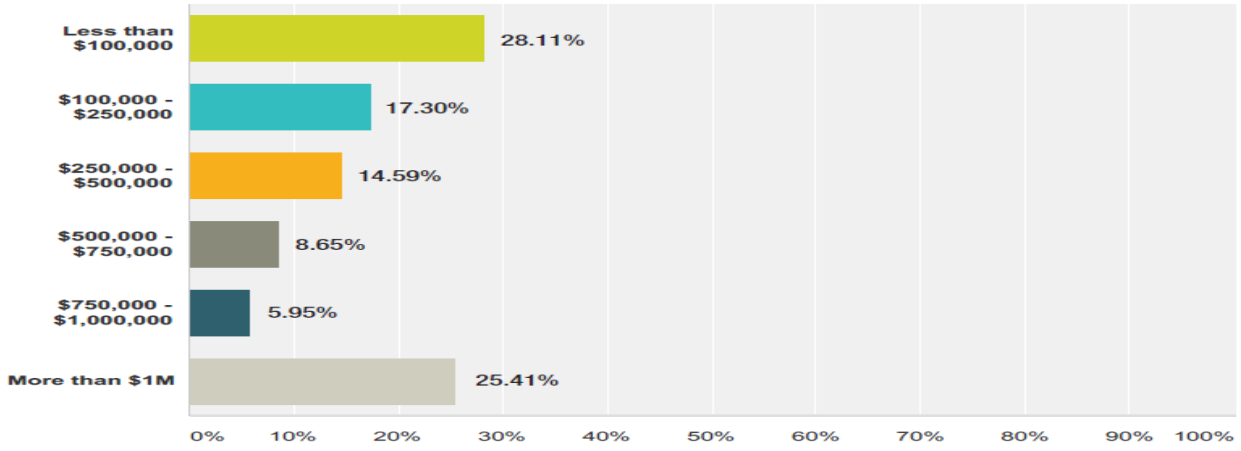
Top 5 Ways Breaches Affected Victimized Companies

Lost reputation, brand value and marketplace image	52%
Lost time and productivity	46%
Cost of purchased technology	38%
Cost of notification	27%
Cost of preventing harm to victims	23 %
Cost of consultants and attorneys	23%

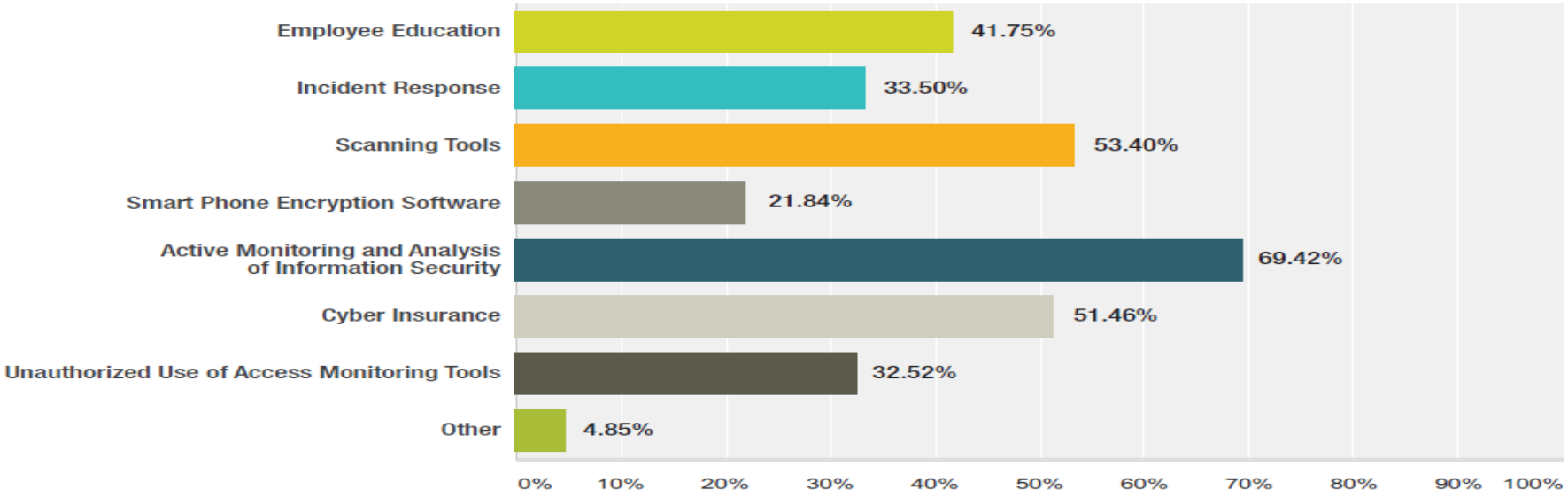
RIMS the risk management society™

Source: Identity Finder and Ponemon Institute, "2014: A Year of Mega Breaches"

QUESTION 21. How much will your company spend to protect cyber security exposures in 2015?



QUESTION 22. What will be your top cyber risk spending categories in 2015? (Please check all that apply)

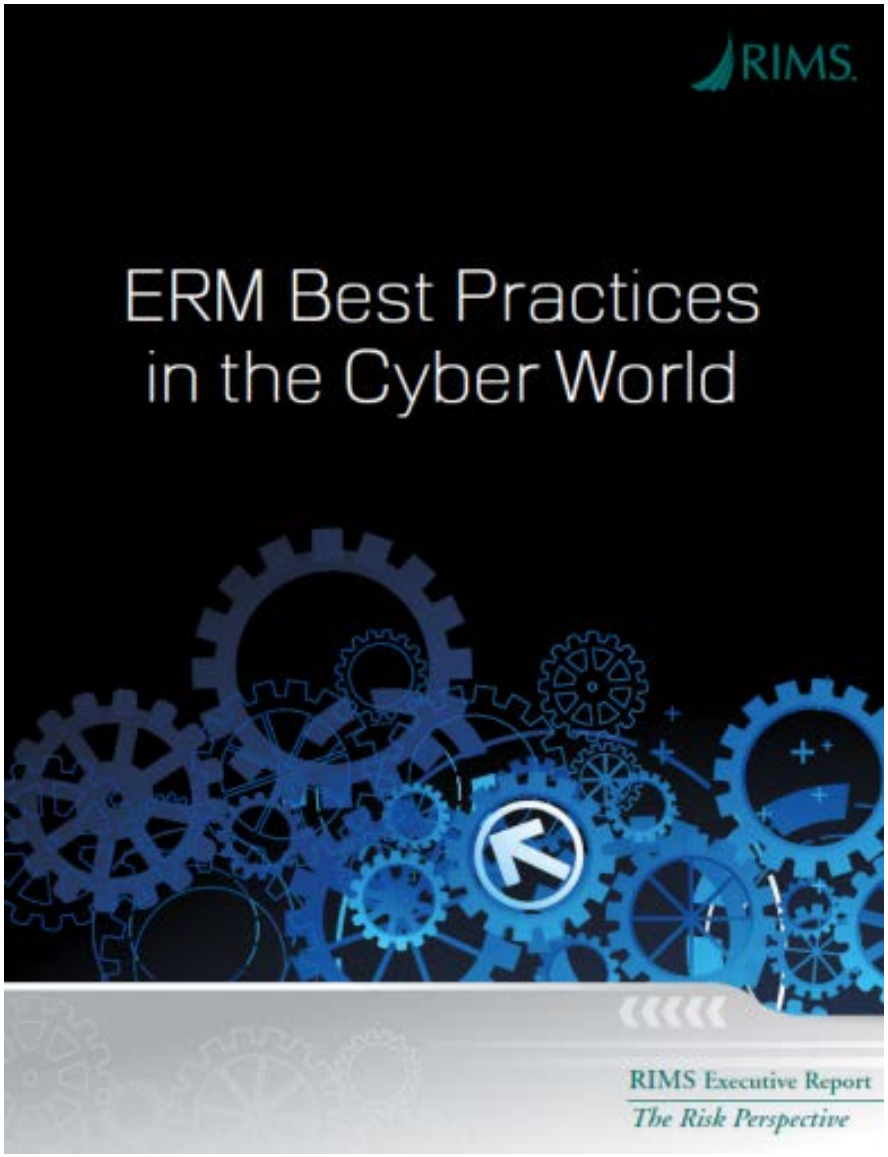


87%

of hackers say that it is just as easy, if not easier, to compromise privileged account credentials as it was two years ago, despite increased corporate cybersecurity spending.

Source: *Thycotic Black Hat 2015 Hacker Survey*

RIMS
the risk management society™



DATA BREACH

An incident (or series of incidents) in which sensitive, protected or confidential information has potentially been viewed, stolen or used by an individual or entity unauthorized to do so.

RIMS
the risk management society™

FORMING A CYBER RISK TEAM

- Technology Leaders
- Legal Advisors
- Select Operational Leaders
- Communications
- Human Resources
- *Outside Resources

RIMS
the risk management society

DOCUMENTING DATA, DATA FLOW AND RELATED PROCESSES

What is the sensitive data (SD)?
- PII
- PHI
- PCI
- Confidential business information
- Intellectual property

What laws & regulations govern this data?
- State laws where we operate (12)
- EU privacy
- HIPPA/HITECH
- PCI-DSS
- VISA/MC/AMEX
- Internal policies

In what form is the SD?
- Client account applications
- Credit bureau info
- Employee records
- Health & insurance
- Attorney litigation files
- Client list & pricing
- Company bank records

Other special considerations?
- Use of off-shored resources (India) for customer service and routine client file maintenance
- Exchange of SD information for M&A due diligence

Who provides sensitive data?
- Customers/clients
- Employees
- Credit card companies
- Banks/financial institutions
- Credit bureaus
- Other businesses

Ways SD comes into business:
- Person
- Computers/mobile
- Website
- Email
- FTP/SFTP
- Mail
- FAX
- Phone
- Cash registers

Where SD is:
- Computers & laptops
- Mainframe/servers
- Disk/tapes/CDs
- Flash drives and portable storage
- Office/home files
- Databases
- Branch offices

Who can access SD:
- Employees
- Customers
- Vendors
- Contractors
- Others

What are the internal threats to the data?
- Misplaced or lost data
- Data sent in error
- Malicious data destruction, manipulation, or alteration
- Employee theft of data
- Vendor theft of data
- Authorized access
- Unauthorized access

What are the external threats to data?
- Theft of trash
- Theft from premises
- Computer hacking
- Spyware & malware
- Access - unintentional disclosure
- Malicious data destruction, manipulation, or alteration

Security controls internal access:
- System access & role based entitlement control
- Admin rights controls
- System audit trail
- Locked down USB port
- VPN remote access
- Employee screening
- Employee training

Security controls external access:
- Building/office security
- Document destruction
- Firewalls
- Updated anti-virus
- Encryption
- Intrusion detection sys.
- Patch management
- Secure wireless
- Penetration testing

Employee SD training:
- Signed confidentiality statement by employee
- "Protecting company confidential information training program"
- New employee orientation includes SD
- Annual training & test
- Quarterly awareness communications

Third party vendor management:
- Internal company vendor management program
- Contracts - appropriate SD considerations
- Due diligence program
- Audit & certifications
- Penetration testing
- Employee training

Security assessment & audit:
- Policies & procedures
- Operations & execution
- Stand-alone technical SA program covers all key areas
- Change management
- Artifact & log review

Data breach:
- Responsibility & ownership assigned
- DB team identified & trained
- Policies & procedures defined & published
- Resources in place
- DB program integrated into the DR/COB program

RULES FOR MANAGING DATA

1. If the organization does not need it, do not collect it.
2. If data must be collected, collect only what is needed.
3. If data is needed, control it and encrypt it.
4. When data is no longer needed, get rid of it, SECURELY.

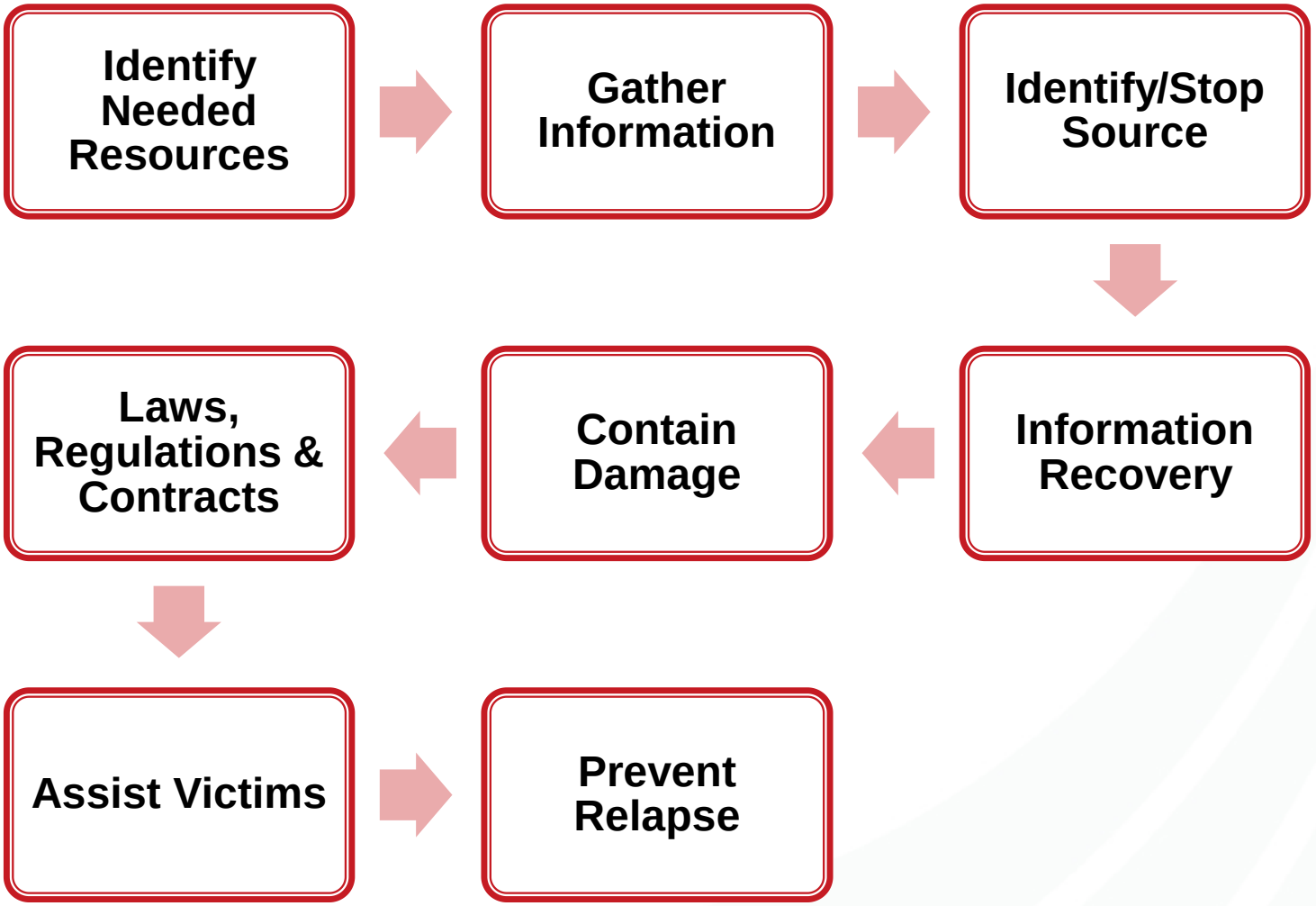
RIMS
the risk management society™

Breach Planning & Response Steps

- ✓ Pre-Planning for Breach
- ✓ Execution of Plan
- ✓ Cyber Team Briefing
- ✓ Investigation and Damage Assessment
- ✓ Remediation and Resolution
- ✓ Computer Forensic Assistance
- ✓ Media Relations
- ✓ Mandatory Breach Notification
- ✓ Monitor Activities and Environment

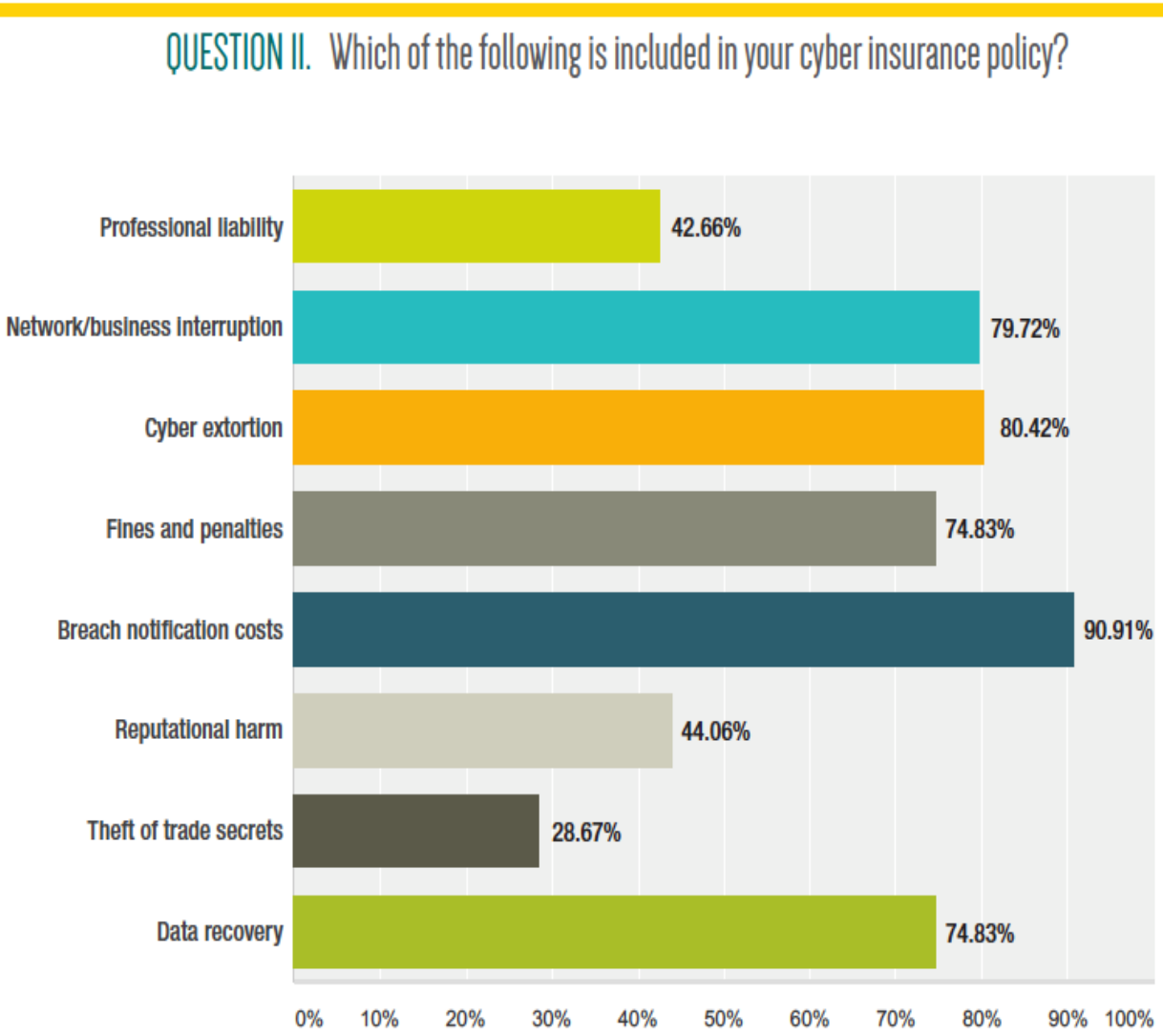
RIMS
the risk management society™

CYBER RISK TEAM ACTION ITEMS:



RIMS the risk management society™

PURCHASING CYBER INSURANCE



RIMS
the risk management society™

STRESS TESTING

Know Your Responsibilities

Know the Escalation Process

Know the Approval Process

RIMS the risk management society

OTHER POST BREACH CONSIDERATIONS

- Review Insurance Policies
- Implement Effective Communications
- Develop Timeline
- Confirm Breach Status
- Establish Accounting Procedures
- Secure Documentation of Losses
- Consider Reputational/Brand Damage

RIMS
the risk management society

SUMMARY:
FUNDAMENTAL STEPS OF A CYBER RISK STRATEGY

Common Terms

Cyber Risk Team

Sensitive Data

Cyber Risk Insurance

Stress Testing

Response Plan

Post-Breach Plan

RIMS
the risk management society

Thank You!

RIMS 16
San Diego | April 10-13

RIMS ERM Conference 2016

OCTOBER 24–25 | W ATLANTA–MIDTOWN | ATLANTA, GA

WWW.RIMS.ORG

RIMS CLIENT SERVICE TEAM: CST@RIMS.org

RIMS the risk management society