Breach of Confidence

Results of the 2009 **Banking Information Security Today**™ Survey – and a Look Ahead at the Issues Shaping 2010

ISMG
INFORMATION SECURITY
MEDIA GROUP

2010: A Look Forward

Banking Information Security Today Survey Results Give us a Glimpse of Next Year's Hot Trends

Tom Field
Editorial Director
ISMG, Corp.

In a lot of ways, this is my favorite time of year.

Not just because of the holidays and the opportunities to reconnect with family and friends. But also because it's the time of year we start looking ahead to the top banking/security trends of the New Year.

And what better way to start this discussion than by reviewing our latest Banking Information Security Today survey results?

On the following pages, you'll see the statistics and analysis from our second annual survey of banking/security leaders, asking them in-depth questions about the issues that matter most – issues such as:

- The economic crisis;
- Heartland data breach aftermath;
- Regulatory compliance;
- Mobile banking;
- And, of course, much more.

It's no surprise that the economy and Heartland dominate this year's discussion. But it is eye-opening to see new insights on mobile banking trends, as well as to hear advice from bankers on how to improve the regulatory examination process.

Join me, please, in going through the latest survey results. Then offer me your feedback: What do you think will be the major issues of 2010?

As always, meet me back here again before long to participate in the 2010 Banking Information Security Today survey – to set the agenda for 2011 and beyond.

Best,
Tom Field

ISMG
INFORMATION SECURITY
MEDIA GROUP

Editorial Staff

Tom Field, Editorial Director
Linda McGlasson, Managing Editor
Upasana Gupta, Contributing Editor
Karyn Murphy, Contributing Editor

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries. This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

Corporate Headquarters:
4 Independence Way
Princeton, NJ 08540
Phone: (800) 944-0401
Email:info@ismgcorp.com

www.ismgcorp.com
www.bankinfosecurity.com
www.cuinfosecurity.com
www.govinfosecurity.com

Contents

Breach of Confidence

Results of the 2009 Banking Information Security Today Survey – and a Look Ahead at the Issues Shaping 2010

"In many ways, the results of the 2008 State of Banking Information Security survey were a dress rehearsal for 2009 and the forces that are shaping 2010."

Executive Summary

The Economy and Heartland

There is no way you can look at the banking landscape in 2009 and not focus on these inextricably linked events.

Starting in the summer of 2008 with the shocking IndyMac Bank closure, the global recession has had a stranglehold on the financial services industry. And we've witnessed seismic changes: The reshaping of the entire investment banking sector, scores of bank/credit union failures, and a new awareness – from the White House to Main Street – that regulatory reform must occur to prevent further abuses such as those that helped hasten this economic downturn.

"In other words, at a time when financial institutions could least afford it … they were forced to assign extra resources to recover from the Heartland breach."

The Heartland Payment Systems breach of an estimated 130 million accounts – the largest breach ever detected -- occurred sometime in 2008, but was announced publicly on Inauguration Day 2009. And, ironically, what that news inaugurated was a new public outcry against such breaches and the toll they take upon banking institutions and customers, as well as a call for new, more stringent security standards to prevent similar incidents.

In other words, at a time when financial institutions could least afford it – especially in terms of customer confidence – they were forced to assign extra resources to recover from the Heartland breach. And these events combined to define the state of banking information security in 2009. It's been the year of recovery – from recession and of trust.

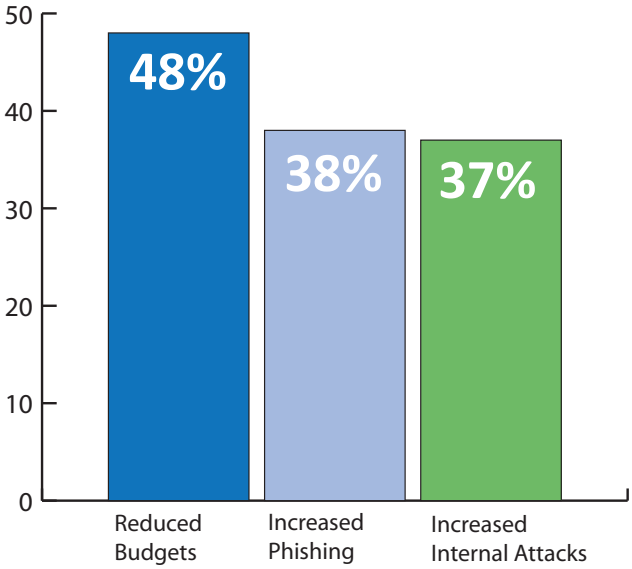
5 Key Themes

Facing 2010, five key themes emerge from our latest annual survey. Each of these themes will be explored in depth in the full report, but for the summary's sake they are:

1: Risks vs. Resources

Because of the recession, institutions are operating with fewer human and financial resources. Yet, security incidents – from the outside and within – are up and demand even greater resources for prevention and remediation.

What has been the biggest impact on information security from the downturn in the economy?'



Then, when asked 'Which security concerns are likely to be part of your main focus?' they said:

Risks Associated with Vendors	60%
Mobile Users/Devices	44%
Insider Fraud	35%

Asked whether insufficient resources are committed to information security and technology risk management, given the rise of security threats and criminal activities against an organization, 52% say yes.

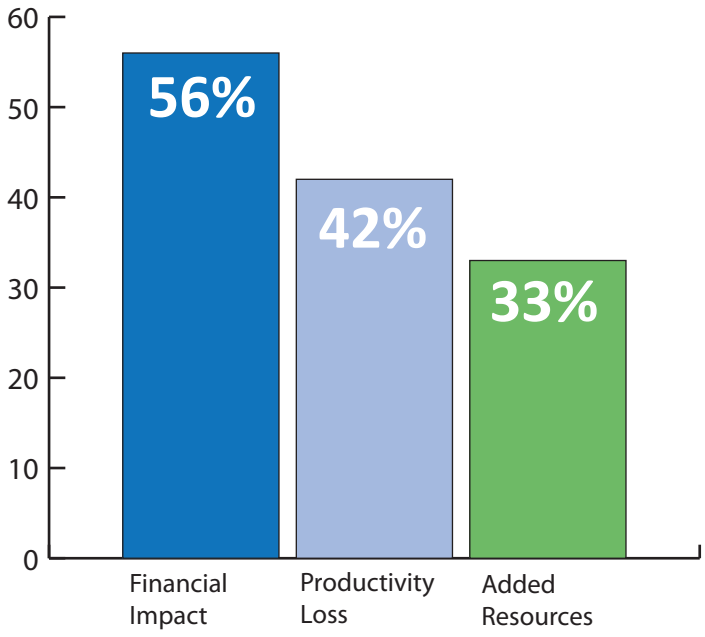
Asked what feeds this perception (which is the institutions' realities), respondents cite three main reasons:

Other business priorities	27%
Economic conditions	25%
Sr. mgt. doesn't understand risks	25%

2: The Heartland Aftermath

It's estimated by attorneys involved in class action suits against Heartland Payment Systems that more than 3,000 banking institutions have been affected by the Heartland data breach. And if this incident has taught us any lessons, then they are: 1) Customers are inclined to 'shoot the messenger' when banking institutions make them aware of card compromises; and 2) Institutions are sick of cleaning up after security disasters that occurred on someone else's (a merchant or a processor's) watch. Among the questions we asked regarding Heartland:

What has been the impact of Heartland-type data breaches?



"56% of respondents report financial impact from the Heartland breach."

What does your institution intend to do to help prevent these breaches?

Educate Customers	58%
Join Industry Groups	51%
Lobby Lawmakers	35%

3: *Real* Vendor Management

This was already a hot button issue before 2009. Through the Identity Theft Red Flags Rule and other guidance, banking regulators made clear to institutions in 2008 that they needed to improve how they selected, contracted with and monitored the security practices of their third-party service providers (TSPs). Then came the Heartland breach and other notable security incidents, which only underscored the inherent risk to data when it's in third-party hands. Our latest survey tells us that institutions do understand the criticality of vendor management. But they still aren't entirely confident in their abilities to do it right. And, in fact, comparing 2008 and 2009 answers, institutions are slipping just a bit. Specifically, we found:

"50% rate confidence in vendors' security controls as medium-to-low."

How do you rate your confidence in your vendor's security controls?

2008 respondents:	46% medium-low
2009 respondents:	50% medium-low

Does your incident response plan account for incidents at vendors?

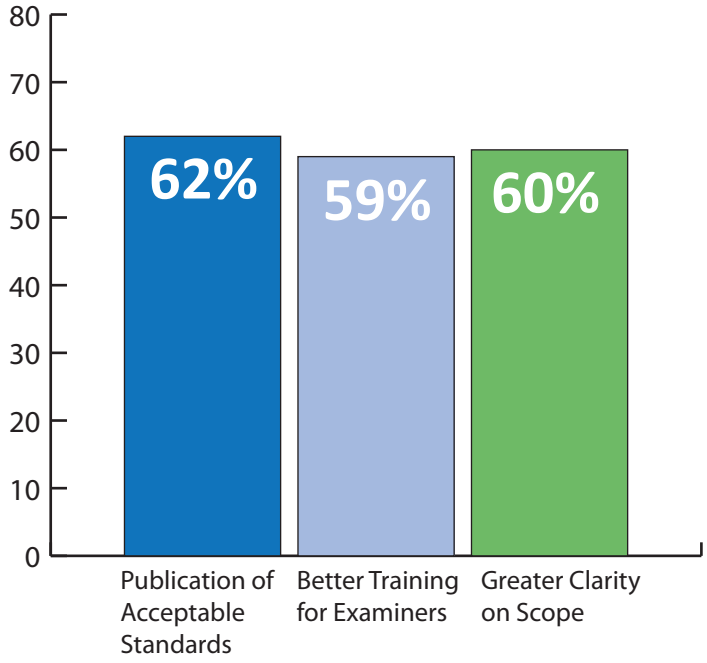
2008 respondents:	55% Yes
2009 respondents:	51% Yes

4: Maximum Compliance

Given the initial attention paid to the Obama Administration's financial rescue plan and selection of a Treasury secretary (before people's eyes veered to healthcare reform), one knew that regulatory compliance would be at center stage in the banking industry in 2009. But we wondered 1) Would regulators be inclined to give institutions a break, in light of economic conditions? And 2) What are the institutions' views on the work that examiners are doing? We hear a lot from regulators about the institutions' practices, but what about the banks' and credit unions' perspectives on the regulators' work? Here's what we learned:

"59% say better training will improve the quality of regulatory exams."

What will improve the quality of technical/operations exams?



On which areas do you wish regulatory agencies focused more attention?

Awareness	38%
Tech/Operations	40%
Auditing, testing	35%
Training	30%

5: New Banking Services/Emerging Technologies

We learned in our 2008 Banking Confidence Survey that, even though resources were tight, institutions continued to invest in mobile banking and other new services that would both attract new customers and retain existing ones. This latest survey tells us exactly where – and why – institutions are investing development dollars.

Will you introduce mobile banking?

Yes/Don't Know	40%

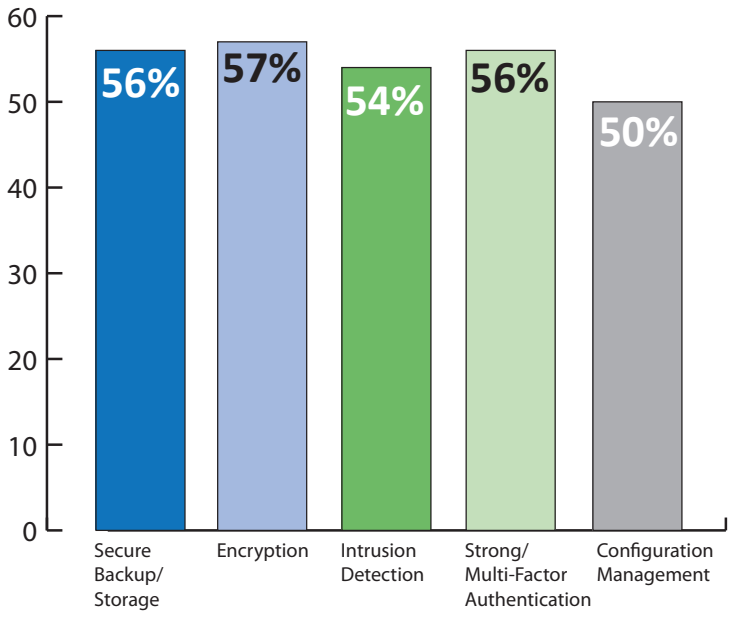
Why?

Attract New Customers	38%
Serve Needs of Existing Customers	37%

Beyond mobile banking, we asked institutions where they would invest time and money in new services and technologies in 2009. In fact, we asked them both 'What will you do?' and 'What do you wish you could do?' Their responses:

"57% will deploy encryption technologies"

Which security services/technologies will you deploy?



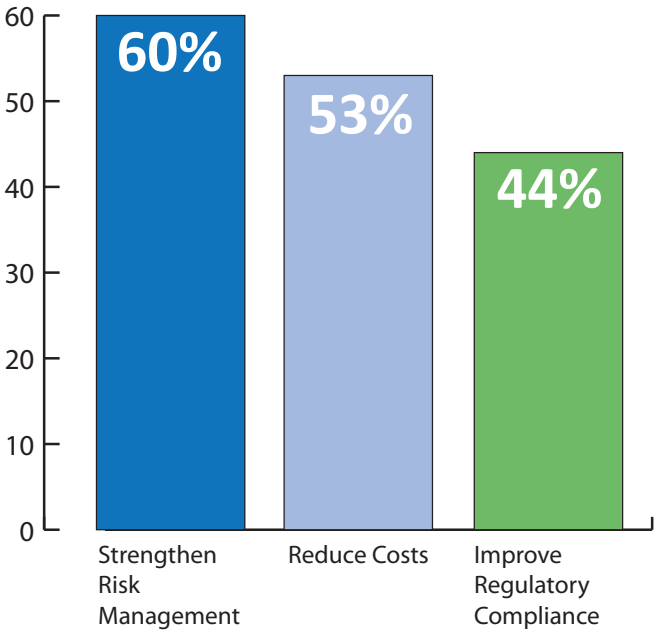
What technologies/goals do you wish your organization had planned for 2009?

Fraud Prevention	40%
Secure PDA's	30%
Secure Endpoint Devices	27%
Secure Document Mgt.	25%
Biometrics	25%

Emerging Storylines

Among the other key agenda items to emerge from this year's survey are:

Spending Priorities: What are your three greatest spending priorities?



2008/2009 Points of Comparison

Reporting relationships and budgets, of course, are key to the success of information security leaders and programs, and so we asked:

Reporting Relationships: Do banking/ security leaders report to CEO/Board?

2008: 41% Yes
2009: 45% Yes

Information Security Budget: Is it Part of IT?

2008: 54% Yes
2009: 45% Yes

Greatest Challenges: What are your biggest challenges to mitigating risks?

Insufficient Budget	38%
Insufficient Resources	37%
Lack of Tools, Technology	33%

"60% cite strengthening risk management as among top spending priorities."

The Year's Agenda

In analyzing the year's survey results, one distinguishes two sets of marching orders – one for the banking community, and another altogether for non-banking entities that look to financial services for information security leadership.

For the banking industry, these truths are clear:

1. Trust is still job #1

Now more than ever, in the wake of the recession and much-publicized data breaches, institutions must redouble their efforts to protect and educate their customers. As recent news reminds us, ACH and ATM fraud incidents are on the rise, and institutions and customers alike must get smarter about thwarting them.

2. Vendor Management is more important than ever

Regulators weren't necessarily talking about payments processors when they hammered home the vendor management message in 2008. But if the Heartland breach reinforces anything, it's that institutions and their customers are at great risk when critical data is insufficiently protected in third-party hands. And we know from tracking fraud trends that processors are increasingly in the fraudsters' target. No longer are individuals the prime targets; the criminals now are after the biggest potential paydays – processors and, ultimately, the credit/debit card companies themselves.

3. Watch the insider threat

Desperate times create desperate people. Witness: Societe Generale and the Countrywide scandals – two of the most public of insider crimes we've seen. Throughout 2009, in the wake of layoffs, foreclosures and increased financial stress, we've seen a rash of insider crimes – especially in financial services, where embezzlement and identity theft incidents have risen. Institutions must take extra care with background checks, and proper monitoring must be in place to catch anomalies as they occur.

4. Regulatory shakeup is coming

President Obama has put forward a plan for the greatest banking regulatory shakeup since the 1930s, and Congressional leaders even now are crafting their own versions. Despite signs of economic improvement, as well as a shift of national attention toward healthcare reform, banking remains a key legislative focus. And we can expect to see increased talk of reform going into 2010. Key questions: Will any of the current regulatory agencies be eliminated or consolidated, as has been suggested? What type of checks-and-balances will be put in place to catch warning signs similar to those that went undetected before 2008's crash?

5. It's time to invest in new customers

Even in the midst of the economic meltdown in late 2008, we found that 40% of surveyed institutions were investing money in mobile banking and other new services. The message: The competition for new deposits is increasing, and to win these accounts institutions are deploying new electronic services that will retain current customers, as well as attract new, younger, more tech-savvy consumers. If you're not investing in these services, it's a safe bet that your competitor is. If you are, then you already know: Vendor management and customer awareness are key elements of ensuring successful programs.

For observers outside of banking, here is what these survey results reinforce:

1. Privacy is primary

if you collect critical data on your customers and their personal information, then protect it with your business' life. Because that is what is at stake. This point is particularly relevant to government agencies, which have suffered some painful breaches, and healthcare organizations, where medical identity theft incidents are on the rise.

2. Know Thy Vendor

Learn from the examples of TJX, Hannaford and Heartland, where financial institutions and their customers have suffered because of misuse of data when it was in the hands of third-party service providers. You must be able to vouch for your vendors' security practices as well as you can your own.

3. Monitor Insider Threat

Again, desperate times create desperate people. 2009 has seen a rash of insider crimes across all industries. These crimes can be just as damaging as an outside attack, yet too often the warning signs aren't just ignored – they're scarcely monitored.

4. Awareness is Key

From the board of directors to your customers, everyone needs to know how you're securing the business. In terms of the board and senior management, it's the law – you are required to keep them aware of security practices. With customers, it's simply good business sense to reinforce what you're doing – and what they can do – to protect their financial and informational assets.

Other Resources

Check Out These Other Reports From ISMG Research

Now in Our Third Year of Offering Unique Industry Insights

If you enjoyed reading this report, please check out these additional surveys from Information Security Media Group:

The State of Banking Information Security 2008

http://www.bankinfosecurity.com/survey.php

Identity Theft Red Flags Rule Compliance Survey

http://www.bankinfosecurity.com/survey_idred.php

Application Security Survey

http://www.bankinfosecurity.com/surveys.php?surveyID=1

Banking Confidence Survey

http://www.bankinfosecurity.com/surveys.php?surveyID=2

Information Security Today: Career Trends Survey

http://www.bankinfosecurity.com/surveys.php?surveyID=6

INFORMATION SECURITY MEDIA GROUP

4 Independence Way | Princeton, NJ 08540
ISMGCorp.com