



# **Cyber Risk Insurance: Policies, Claims and Coverage**

Seton Hall University School of Law

Jennifer Rothstein

February 24, 2015

# Trends in Data Security

- Trends
  - Data breaches
  - Data dams
  - DDoS attacks
  - Ransom ware
  - Malware, malware, malware ...
  - Attacks on all sectors



# Ransomware

- Ransomware is malware used for data kidnapping, an exploit in which the attacker encrypts the data and demands payment for the decryption
- Ransomware attacks can come with other malware

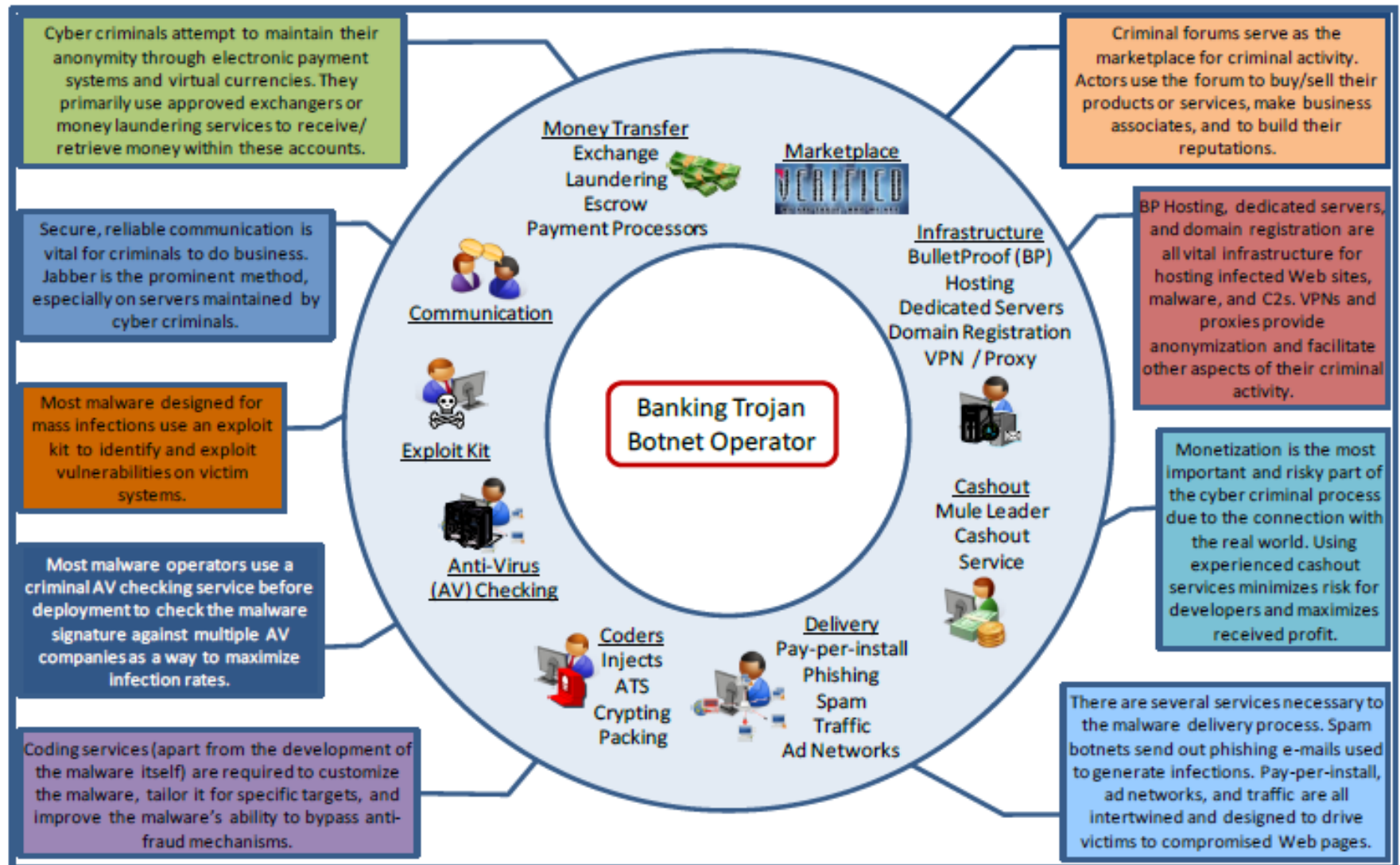


# Who is in the Headlines Today?

The collage features several overlapping elements:

- Bloomberg Businessweek Technology** banner with navigation links: Global Economics, Companies & Industries, Politics & Policy, Technology, Markets.
- THE WALL STREET JOURNAL** banner with a "MARKETS" tab.
- TOP STORIES IN MARKETS** section with three articles:
  - 1 of 12: Investors Should Fear Fed's Rate Shadow (with image of the US Capitol)
  - 2 of 12: Margins Give Mattress Firm More Bounce
  - Big Banks Won't Drown Liquidity Rule
- MARKETS** section with the headline: **FBI Probes Possible Hacking Incident at J.P. Morgan** and sub-headline: **Attack Appears to Have Been Caused By Malicious Computer Code**.
- info security** banner with navigation links: Strategy, Insight, Technology, News, Topics, Features, Webinars, White Papers, Jobs, Events & Conferences, Directory. It includes a "Latest" article: "How Cyber-smart Are You? Kaspersky, Mensa Put It to the Test".
- Krebs on Security** banner with the tagline "In-depth security news and investigation".
- 03 Data: Nearly All U.S. Home Depot Stores Hit** headline.
- mail** button on a keyboard.
- 2 SEP 2014 | NEWS** headline: **Russian Gang's Billions of Stolen Credentials Resurface in New Attack**.

# The Cyber Underground ...





# Preparation for a Breach: High Breach Costs

U.S. average per capita cost of data breach (cost per record)

**\$201**

U.S. average cost of a data breach

**\$5.85 mln**

World average cost of a data breach

**\$3.5 mln**

Annual increase in the average cost of a data breach around the world

**15%**

Source: 2014 Cost of Data Breach Study: Global Analysis  
Sponsored by IBM, Conducted by Ponemon Institute LLC

# Consumer Cybercrime Across the Globe

**378M**

Cybercrime  
victims per year

**1M+**

Cybercrime  
victims per day

**12**

Cybercrime  
victims per  
second

**\$113B**

Cost of  
cybercrime  
annually

**\$13B**

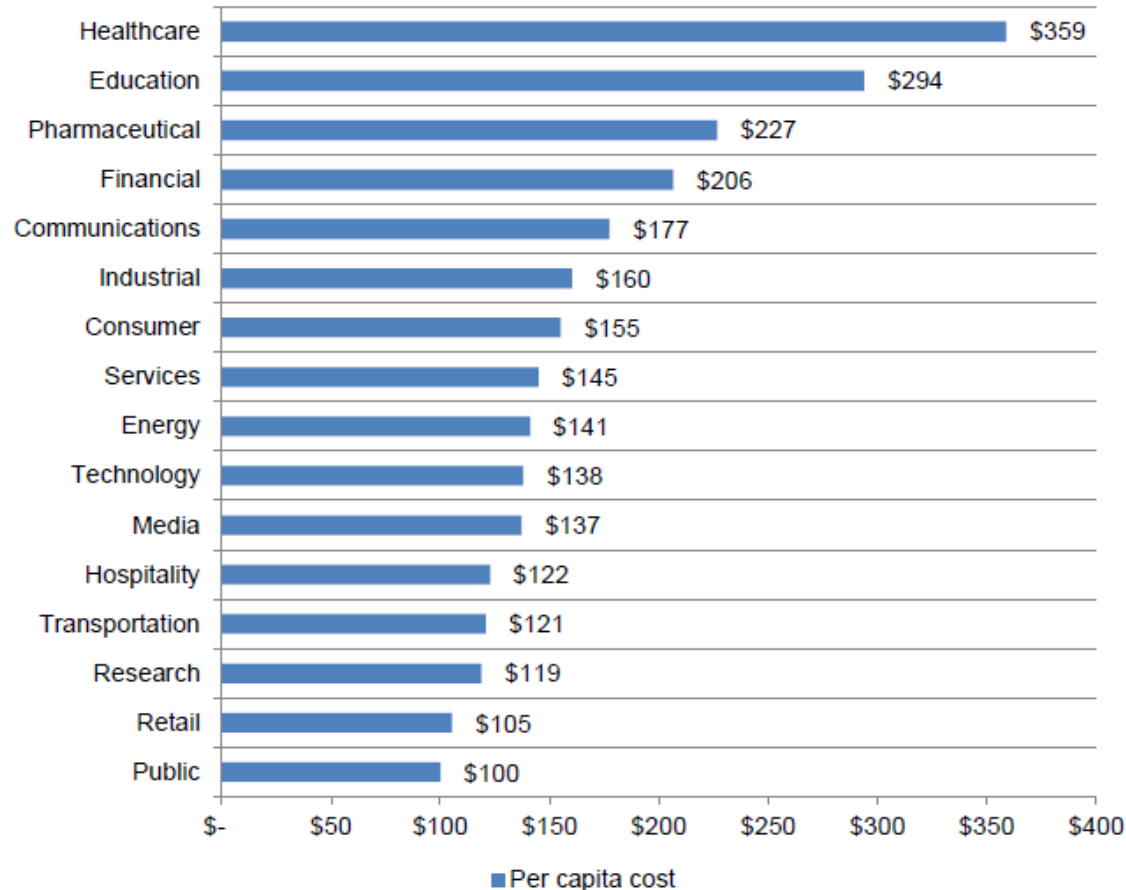
Cost of cybercrime  
annually in Europe

(2013 Norton Cybercrime Report)

# Preparation for a Breach: High Breach Costs

**Figure 4. Per capita cost by industry classification**

Consolidated view (n=314)



Source: 2014 Cost of Data Breach Study: Global Analysis  
Sponsored by IBM, Conducted by Ponemon Institute LLC



# Preparation for a Breach: a Vulnerable Sector

## Data Breach Incidents by Sector, 2013


Source: Norton Cybercrime Index

Industry Sector	Number of Incidents	Percentage of Incidents
Healthcare	93	36.8%
Education	32	12.6%
Government and Public Sector	22	8.7%
Retail	19	7.5%
Accounting	13	5.1%
Computer software	12	4.7%
Hospitality	10	4.0%
Insurance	9	3.6%
Financial	9	3.6%
Transportation	6	2.4%
Information technology	5	2.0%
Telecom	4	1.6%
Law enforcement	4	1.6%
Social networking	3	1.2%
Agriculture	2	0.8%
Community and non-profit	2	0.8%
Administration and human resources	2	0.8%
Military	2	0.8%
Construction	1	0.4%
Utilities and energy	1	0.4%
Computer hardware	1	0.4%

Internet Security Threat Report 2014: Volume 19, Appendix A; Symantec Corporation

# Cost Factors

## Factors that decreased the cost of a data breach

- 
- Strong security posture
  - Incident response planning
  - Business continuity management
  - CISO appointment

## Factors that increased the cost of a data breach

- 
- Lost or stolen devices
  - Third party involvement
  - Notification before investigation completed

Source: 2014 Cost of Data Breach Study: Global Analysis  
Sponsored by IBM, Conducted by Ponemon Institute LLC

# Preparation for a Breach: Frequency Per Sector

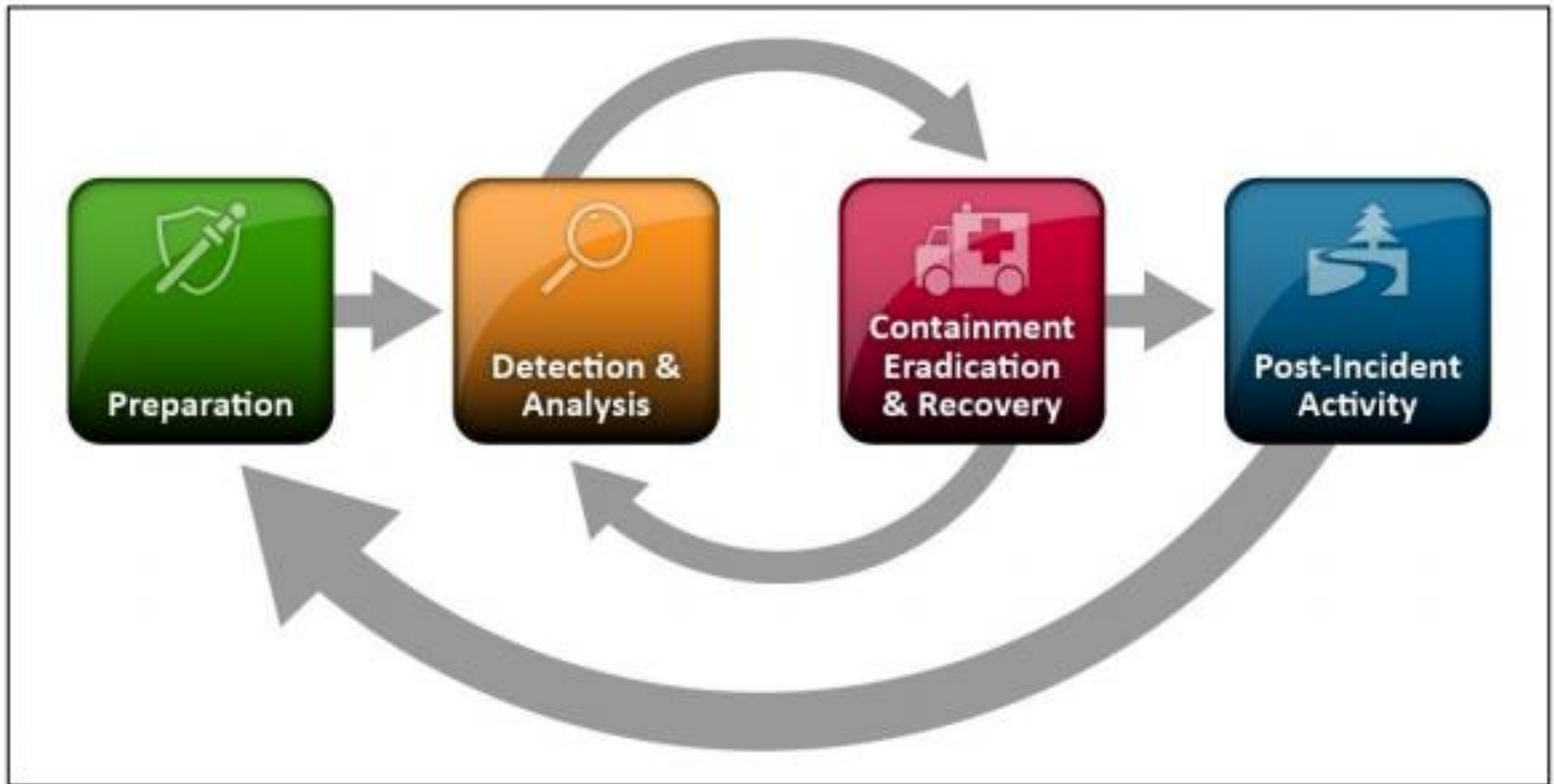
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31.32.33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44.45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48.49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

For more information on the NAICS codes [shown above] visit: <https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012>

2014 Verizon Data Breach Investigations Report

# Information Security Incident Cycle



Computer Security Incident Handling Guide, NIST SP 800-61 Rev. 2

# Update Security Posture

- Use current version of operating systems if possible
- Automate operating system security patching
- Automate security application patching
- Employ white listing
- No local administrative control
- Segregate network using domain controls
- Use multi-factor authentication
- Eliminate unnecessary processes
- Eliminate unnecessary data
- Endpoint monitoring
- Due diligence on all third party service providers
- Conduct risk assessments

# Have Fire Drills

- Pen testing of POS system
  - Review of actual network operations to detect vulnerabilities
- Internal control review
  - Review written policies, protocols & certifications
  - Verify implementation of PCI-DSS
- Legal review
  - Compliance with PCI
  - Policy coverage
  - Banners and notices
- Table top exercises
  - “fire drill” a POS attack
    - Test the team
    - See how crisis unfolds
    - Hands on response



# The Initial Response

- Conduct a quick assessment
  - If possible breach - implement incident response plan
  - Do not wait until 'verified'
- Notify insurer
  - Confirm approval of all breach vendors
- Engage outside counsel
- Engage digital forensics team through counsel
- Implement litigation hold

# Anatomy of a Breach:

## Containment/Eradication/Recovery

- Deploy forensics firm to assess, contain, eradicate, analyze and remediate
  - Identify target of breach, i.e. PHI, intellectual property, payment card systems, financial account information, etc.
  - Determine whether data loss occurred, if so, whether it has stopped
  - Eliminate threat
  - Determine extent of loss
- Preserve and secure evidence, including all log files
- Recovery – return affected systems to normal operations

# Consumer Services Decision Factors

## 1. How did the data breach occur?

- High, Medium or Low Risk based upon an investigation

## 2. How many people were impacted and where do they live?

- Size of the event may often define what solutions are available to be used
- Location of the population may expose a higher propensity to becoming a victim of identity theft

## 3. What type of PII/PHI was exposed?

- Financial? Medical? What services actually address the exposure?

## 4. Who is the impacted population?

- VIPs, Clients, Employees, Deceased, Minors, Elderly, Ex-pats?

# Consumer Services Decision Factors

## 1. How did the data breach occur?

- High, Medium or Low Risk based upon an investigation
  - A hacked server where customer PII is stored = high risk
  - A thumb-drive lost at the airport = medium risk
  - A lost laptop that's fully-encrypted = low risk



# Consumer Services Decision Factors

## 2. How many people were impacted and where do they live?

- Size of the event may define what solutions are available to be used
- Location of the population may expose a higher propensity to becoming a victim of identity theft





















































































<http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>

Identity Theft Complaints			
Rank	Victim State	Complaints per 100,000 Population	Complaints
1	Florida	192.9	37,720
2	Georgia	134.1	13,402
3	California	105.4	40,404
4	Michigan	97.1	9,606
4	Nevada	97.1	2,708
6	Maryland	95.5	5,660
7	Arizona	91.2	6,043
8	Texas	88.0	23,266
9	New York	86.9	17,072
10	Illinois	85.9	11,069

# Consumer Services Decision Factors

## 3. What type of PII/PHI was exposed?

- Financial? Medical? What services actually address the exposure?

		Breached Data	Fraud Risk	Recommended Remediation Services				
		Type of PHI/PII exposed:	Specific identity theft and fraud risk associated with exposed PHI/PII:	Advisory Services/ Identity Recovery	Internet Monitoring	Public Records Monitoring	Specialty Reporting Agency Monitoring	Credit and Credit Monitoring Services
Primary Identifiers	SSN + Name, Address or DOB	      						
	Credit Card #s	      						
	Banking and Financial Account #s	      						
Secondary Identifiers	Insurance #s	      						
	Medical ID #s and related PHI	      						
	Driver's License #s	      						
	User Account Log in Information (including email)	      						



# Consumer Services Decision Factors

## 4. Who is the impacted population?

- VIPs, Clients, Employees, Deceased, Minors, Elderly, Ex-pats?
  - No credit monitoring for minors, some ex-pats or deceased



# Anatomy of a Breach: Post-incident Activity

- Determine whether to notify law enforcement
- Determine whether breach notification is required
- If breach notification is required
  - Determine whether remediation services will be provided
  - Draft notification letters and frequently asked questions
  - Send notification letters to affected consumers and regulatory officials
- Prepare for post-incident regulatory response
- Conduct post-incident debrief