Incident Response Planning Program: *Legal, Insurance, Information Security and Public relations*

CBW
Community Bankers of Washington
"the family of community banks"

Incident Response Planning Program

- Customized services to provide individual analysis and planning for your bank, resulting in a functional incident response plan
  - Two hour cyber liability insurance review
  - Two hour legal consultation on incident response preparedness, including breach notification obligation analysis
  - Two hour coaching session on facilitating crisis communication plan
  - Two hour consultation on technical incident detection, including information security incident table-top test

Incident Response – Best Practices

- Management Response
  - Internal Incident Response Team
  - External Incident Response Team
- Internal Communications Plan
- External Communications Plan
- Contacting Regulators

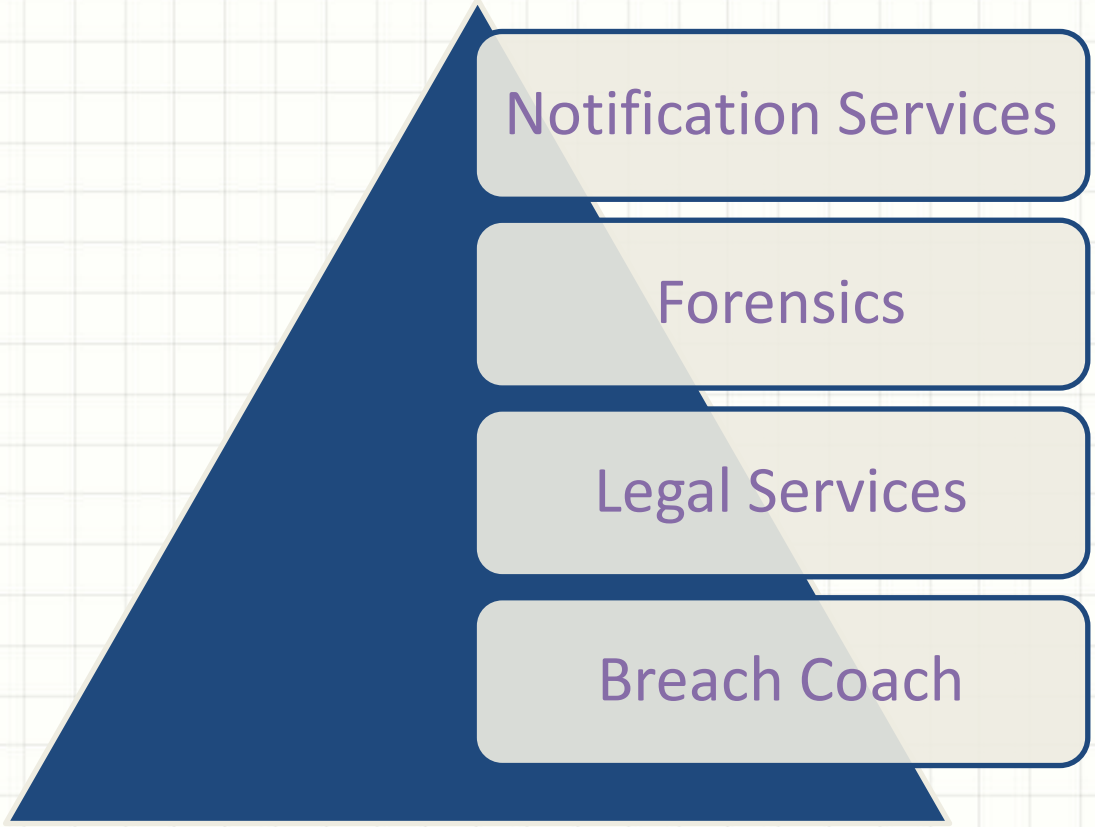
Insurance Coverage for Data Breach Events

- Insurance Trends
  - Exclusions for failure to maintain security standards.
  - Data breaches continue at an alarming rate.
  - Coverages mixed between bond and cyber (beware of ala carte).
  - Limits & Sub-limits
  - Value in post breach response coverage.

Insurance Coverage for Data Breach Events

- First Party Coverage
  - Damage to digital assets
  - Business interruption
- Third Party Coverage
- Extortion
- Remediation
- Regulatory liability
- Privacy liability
  - Network security liability
  - Internet media liability
  - Contractual liability

Cyber Coverage = Access to Resources



Factors When Considering Policy Limits

- What type of data does the bank have?
- How many records does the insured have?
- Does the cyber policy have separate limits or are the limits shared with other coverages (management liability, employment liability, professional liability)?
- Size and location of the insured and its customers.
- Customer profile.
- Regulatory Considerations

7

Risk Shifting by Agreements with Third Party Vendors

- Understand where data resides
- Understand who has access
- Understand liability typically follows the owner of the data
- Establish relationships externally or internally to prepare for pre- and post-breach
- Clarify terms in contractual arrangements:
  - vendor will indemnify / hold harmless; or
  - vendor will maintain cyber insurance.

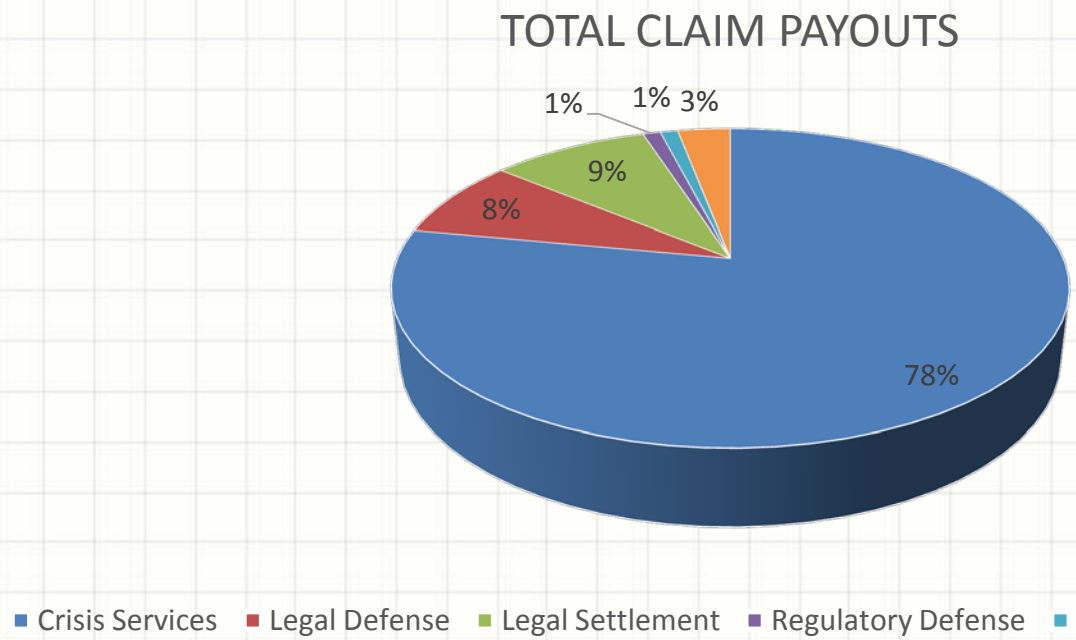
Where are the threats?

- Inside threats
  - Employee negligence
    - Security failures
    - Lost mobile devices
  - Employee ignorance
    - Improper disposal of personal information (dumpsters)
    - Lack of education and awareness
  - Malicious employees
- Outside threats
  - Hackers
    - Malware
    - Phishing and Spear Phishing
  - Thieves (including Social Engineering Tools)
  - Vendors

Average breach claim costs

Lost business	$3.72M
Notification	$560k
Post breach	$1.64M
Detection	$610k
Legal defense	$698k
Legal settlement	$558k

Claims Expenses



Crisis Services

- Forensics
- Notification
- Credit / Id monitoring
- Breach Coach
- Public Relations

NetDiligence 2015 Cyber Claims Study

But It's "Just" a Lost Laptop…

- A Ponemon Institute study indicates that business travelers are losing over 10,000 laptops every week at 36 of the largest U.S. Airports
  - Only 1/3 of them are reclaimed
- More than 53% of business travelers polled say their laptops contain private or confidential information
- Further, 65% admit they do not take precautions to secure the information on their laptop
- Average value of a lost laptop is around $50,000
  - Replacement cost, detection, forensics, data breach, lost IP costs, lost productivity, and legal, consulting and regulatory expenses

Trends in Data Security

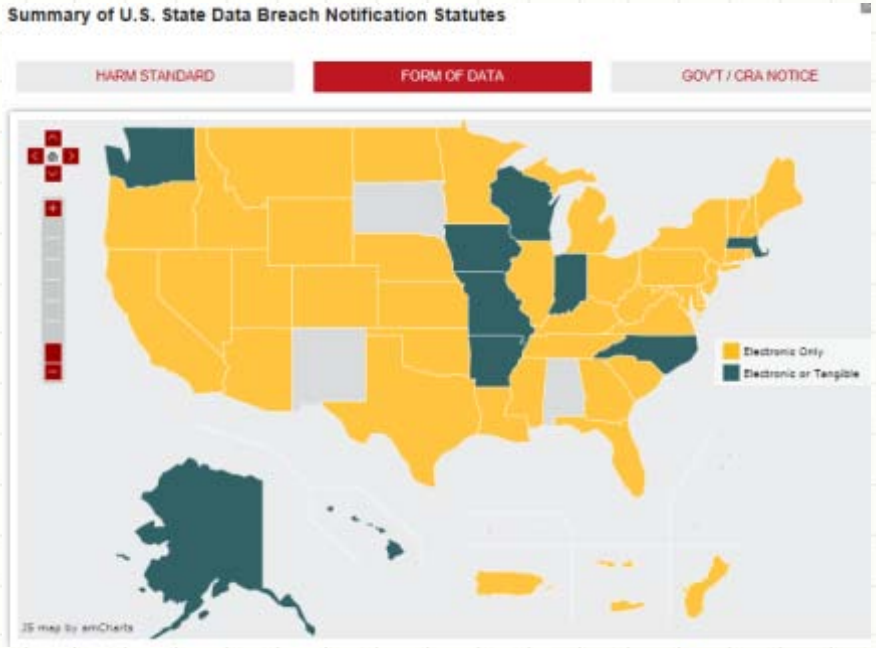
Trends

- Data breaches
  - Databases
  - POS systems
  - Data theft – digital & paper
- Data dams
  - DDoS attacks
- Social engineering
  - Ransomware
  - Fraudulent money transfers
- Malware, malware, malware …
- Attacks on all sectors and all systems

Know your notification obligations

The regulatory environment …

- State Regulations
  - **47 state data breach notification statutes** (plus Washington D.C., Guam, Puerto Rico, and the Virgin Islands)
  - **Require notification of consumers** regarding breaches of unencrypted personal information; 1 requires notification even of encrypted information
  - Notification obligation **determined by residential location of consumer**, not location of business
  - **Personal information** generally defined as first name or initial and last name, combined with one or more of the following data sets:
    - SSN, DL or State ID Card Number, financial account with means to access the account
  - Range of definitions of personal information
    - All include SSN, DL, financial account
    - 8 add medical information
    - 5 add online credentials
    - 13 add other information, including health care, biometric, and taxpayer ID
  - 40 require "most expedient time possible;" 7 also have outer time limit
  - 36 use "harm" and 11 use "acquisition" trigger
  - 19 have specific notice content requirements
  - 25 require notification of state regulatory officials

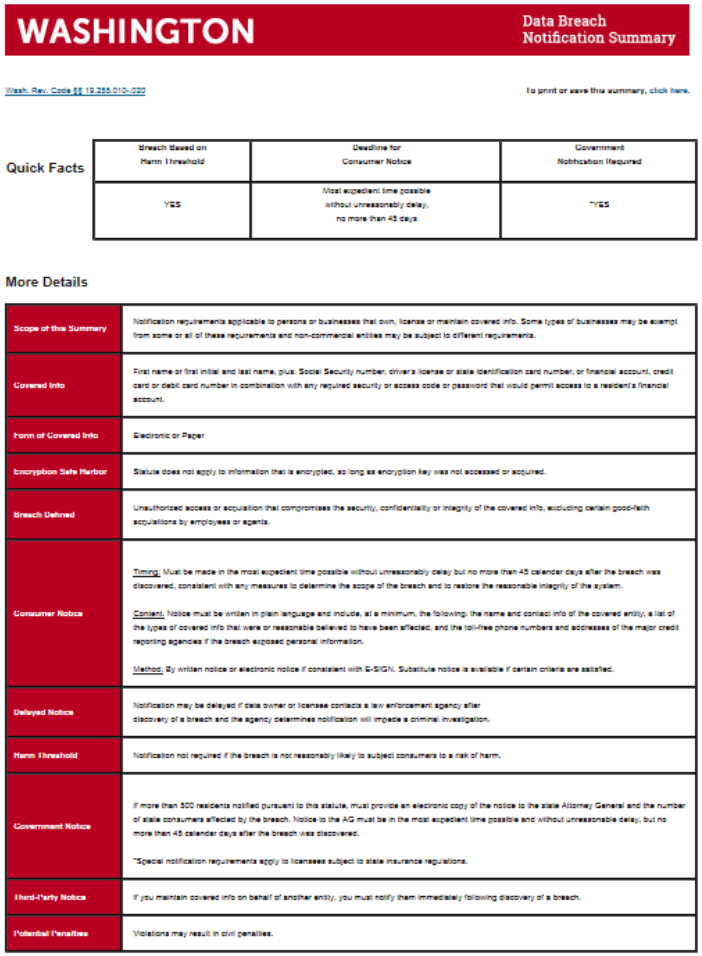


http://www.dwt.com/statedatabreachstatutes

Know your notification obligations

The regulatory environment …

- Washington State Data Breach Notification Statute
  - **Personal information** defined as first name or initial and last name, combined with one or more of the following data sets:
    - SSN, DL or State ID Card Number, financial account with means to access the account
  - **Notice** must be provided in "most expedient time possible" but no more than 45 days from discovery of breach
  - Applies to both **electronic and paper data**
  - Includes a harm threshold, in that notification is not required if the breach is not reasonably likely to subject consumers to risk of harm
  - **Requires notice** to be written in plain language, and to include contact information for covered entity, list of affected data sets, and contact information for credit reporting agencies if sensitive data affected
  - Requires notice of **Attorney General** if more than 500 Washington residents affected



WASHINGTON — Data Breach Notification Summary

Wash. Rev. Code §§ 19.255.010-.020

To print or save this summary, click here.

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
YES	Most expedient time possible without unreasonably delay, no more than 45 days	*YES

More Details

Scope of this Summary	Notification requirements applicable to persons or businesses that own, license or maintain covered info. Some types of businesses may be exempt from some or all of these requirements and non-commercial entities may be subject to different requirements.
Covered Info	First name or first initial and last name, plus: Social Security number; driver's license or state identification card number; or financial account, credit card or debit card number in combination with any required security or access code or password that would permit access to a resident's financial account.
Form of Covered Info	Electronic or Paper
Encryption Safe Harbor	Statute does not apply to information that is encrypted, so long as encryption key was not accessed or acquired.
Breach Defined	Unauthorized access or acquisition that compromises the security, confidentiality or integrity of the covered info, excluding certain good-faith acquisitions by employees or agents.
Consumer Notice	Timing: Must be made in the most expedient time possible without unreasonably delay but no more than 45 calendar days after the breach was discovered, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system. Content: Notice must be written in plain language and include, at a minimum, the following: the name and contact info of the covered entity; a list of the types of covered info that were or reasonable believed to have been affected; and the toll-free phone numbers and addresses of the major credit reporting agencies if the breach exposed personal information. Method: By written notice or electronic notice if consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Delayed Notice	Notification may be delayed if data owner or licensee contacts a law enforcement agency after discovery of a breach and the agency determines notification will impede a criminal investigation.
Harm Threshold	Notification not required if the breach is not reasonably likely to subject consumers to a risk of harm.
Government Notice	If more than 500 residents notified pursuant to this statute, must provide an electronic copy of the notice to the state Attorney General and the number of state consumers affected by the breach. Notice to the AG must be in the most expedient time possible and without unreasonable delay, but no more than 45 calendar days after the breach was discovered. *Special notification requirements apply to licensees subject to state insurance regulations.
Third-Party Notice	If you maintain covered info on behalf of another entity, you must notify them immediately following discovery of a breach.
Potential Penalties	Violations may result in civil penalties.

http://www.dwt.com/washington

Know your regulatory landscape

The regulatory environment …

- Federal Regulations
  - CFPB, FDIC, FFIEC, FTC, FCC, GLBA, HHS/OCR, SEC, OCC, etc.
- Industry Regulations
  - PCI DSS
- Third party liability
  - Class Actions
  - Derivative Suits

Understand the costs of a breach

- **First-party costs**:
  - data loss; software loss; hardware loss;
  - income loss; business interruption costs; restoration costs;
  - cyber extortion; other crime loss;
- **Third-party costs:**
  - media liability (copyright and trademark infringement); privacy liability for breach of privacy; bodily injury;
  - defensive litigation: class actions; derivative actions; and regulatory actions.
- **Remediation costs**:
  - legal services; forensics services; crisis management services; consumer and regulatory notification – the actual hard copy costs; call center services; credit monitoring and identity theft protection services.
- **Fines and penalties**:
  - expenses of regulatory investigations; civil judgments; fines and penalties levied by regulatory authorities; and fines and penalties for payment card industry compliance violations.

Increase Security, Decrease Cost

Factors that decrease the cost of a data breach

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

Factors that increase 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

What Can You Do?

- Security is a marathon, not a sprint
  - take one step at a time … but keep moving forward
- Develop an information security program
  - Administrative measures
    - Slide Communication Plan
  - Technical measures
  - Physical measures
- Be aware of your digital environment
- Be aware of your physical environment

Essential Elements of a Security Program

- Identify and implement an information security framework (e.g. Center for Internet Security Critical Security Controls)
- Assess whether all applicable controls are enabled
- Create and implement information security policies based upon applicable security controls
- Create an incident response plan
- Test the incident response plan through table top exercises
- Conduct regular penetration testing on information system
- Conduct regular review of controls, policies, and incident response plan to ensure all necessary action is being taken

Information Security Controls Managed by the Center for Internet Security ("Reasonable" Security Practices)

- CSC 1 – Inventory of authorized and unauthorized devices
- CSC 2 – Inventory of authorized and unauthorized software
- CSC 3 – Secure configurations for hardware and software on mobile devices, laptops, workstations and servers
- CSC 4 – Continuous vulnerability assessment and remediation
- CSC 5 – Controlled use of administrative privileges
- CSC 6 – Maintenance, monitoring, and analysis of audit logs
- CSC 7 – Email and web browser protection
- CSC 8 – Malware defenses
- CSC 9 – Limitation and control of network ports, protocols, and services
- CSC 10 – Data recovery capability
- CSC 11 – Secure configurations for network devices such as firewalls, routers, and switches
- CSC 12 – Boundary defense
- CSC 13 – Data protection
- CSC 14 – Controlled access based on the need to know
- CSC 15 – Wireless access control
- CSC 16 – Account monitoring and control
- CSC 17 – Security skills assessment and appropriate training to fill gaps
- CSC 18 – Application software security
- CSC 19 – Incident response and management
- CSC 20 – Penetration tests and red team exercises

Data Breach Life Cycle

Access the Problem

- Discover breach
- Contain losses, secure area
- Alert preparedness team
- Notify Insurer
- Notify law enforcement
- Notify regulators

Engage External Resources

- Alert vendor
- Call forensics team
- Alert public relations (internal or external)

Comply with Notification

- Draft and send notification
- Active call center
- Public disclosure (if appropriate)

Manage Ongoing Business

- Continue assuring customers
- Continue data systems monitoring
- Resume business as usual

22

Key Takeaways

- Every system is vulnerable
- Bad guys are:
  - Persistent
  - Well-resourced
  - Increasingly sophisticated
- Increase your security system
- Prepare for the inevitable incident

23

Key Takeaways

- Understand your exposure
- Understand where data resides
- Understand liability falls with the owner of the data
- Establish relationships externally or internally to prepare for pre and post breach

24

Key Takeaways

- Know your Internal and External Resources
- Internal – People responsible
- External
  - Outside Experts
  - Insurance program
    - Know your limits
    - Review policy and limits annually
    - Know how to report a claim
    - Know how to interact with the insurance company

25