Eleventh National HIPAA Summit

5.04 Security Incident Response – What to do if a breach occurs and how to mitigate damages

Chris Apgar, CISSP

Overview

- Background
- Establishing a security incident response team

- Forensics or how to investigate a breach
- Follow up or how to mitigate damages
- Summary & resources

Background

- HIPAA requirements
- Establishing policies and procedures
- Importance of documentation
- Mitigation of legal and regulatory risks
- Sound security practices

Establishing a Security Incident Response Team

- What is a security response team?
- Designing the program
- Corporate buy in
- Determining size of team based on policy and process requirements
- Establishing the team

Establishing a Security Incident Response Team

- Establishing a chain of command
- Supporting policies and procedures
- Designating a team lead
- Responsibilities of the team and team lead
- Training the team

Establishing a Security Incident Response Team

- Establishing a support structure in the organization
- Mapping out process and external resources
- What external resources may be needed?
- Relation to disaster recovery plan

Forensics or How to Investigate a Breach

- Stop any further breach
- Solving the “crime”
- Importance of creating an evidence trail
- Importance of creating un-impeachable evidence

Forensics or How to Investigate a Breach

- Investigating the breach
- Duties of the incident response team
- Establishing a command center
- Determining type of breach
- Determining if truly a breach or a malfunction of software/hardware

Forensics or How to Investigate a Breach

- Tracing the breach to its source
- Internal versus external breach – hacker versus employee
- Actions to be taken based on source of breach
- Regulatory requirements in some states

Forensics or How to Investigate a Breach

- A word about investigations
- Treat a breach as if you were a detective
- If criminal activity is present following proper forensic procedures is extremely important
- When is it necessary to call in the police, FBI, etc.?

Forensics or How to Investigate a Breach

- Use of external organizations to conduct investigations
- Advantages of external resources to smaller organizations
- Use of external resources does not mean it replaces at least a small incident response team
- Best to contract in advance of any incident

Follow Up or How to Mitigate Damages

- A word about mitigating damages
- Importance of proper backup and recovery processes
- Don’t forget proper forensics – keep a copy of the data in question before restoring safeguards, data, etc.
- Coordinate with incident response team

Follow Up or How to Mitigate Damages

- Fast action results in lower mitigation requirements
- Assess damage to data, hardware, software
- Coordinate with appropriate organizational representatives but keep the list short
- Determine if privacy breach also occurred

Follow Up or How to Mitigate Damages

- Determine whether to notify members or patients of any privacy breach
- Be aware of state reporting requirements (especially California)
- Avoiding adverse publicity
- Proactively responding if adverse publicity occurs

Follow Up or How to Mitigate Damages

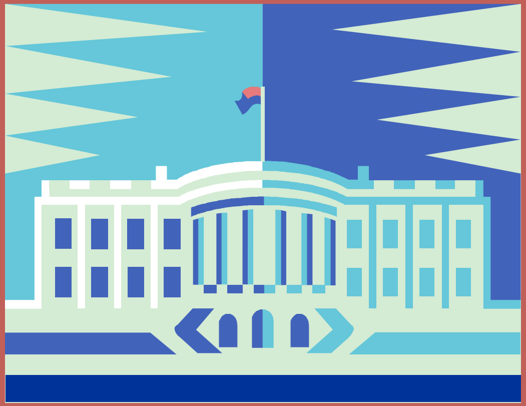
- Limiting litigation or legal risk
- Limiting regulatory risk
- Why or why not report incidents to the authorities
- Internal versus external exposure

Follow Up or How to Mitigate Damages

- Internal versus external perpetrator
- Involving Human Resources
- Sanctions – consistency a must
- Determining the audience – who should I tell?
- Steps to limit future threat of similar nature

Follow Up or How to Mitigate Damages

- No requirement to report breach to OCR or CMS but state laws may require reporting
- What if CMS or OCR investigates?
- Importance of policies and procedures
- Check your contracts – do they require any specific reporting and when
- Returning to normal



Summary

- Establish incident response team before incidents occur
- The importance of forensics
- Importance of consistency and limiting exposure
- Fast reaction limits damages and mitigation costs
- Beware of regulatory, legal and public exposure

References

- NIST Special Publication 800-61: http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf
- SANS: http://www.sans.org
- ISSA: http://www.issa.org
- WEDI: http://www.wedi.org/snip

References

- Handbook for Computer Security Incident Response Teams (Carnegie Mellon): http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html
- FCC Computer Security Incident Response Guide: http://csrc.nist.gov/fasp/FASPDocs/incident-response/Incident-Response-Guide.pdf
- ISS Computer Security Incident Response Planning: http://documents.iss.net/whitepapers/csirplanning.pdf

Q&A

Chris Apgar, CISSP
President
Apgar & Associates, LLC
10730 SW 62nd Place
Portland, OR 97219
(503) 977-9432 (voice)
(503) 816-8555 (mobile)
Capgar@easystreet.com
http://www.apgarandassoc.com