Steptoe
STEPTOE & JOHNSON LLP

Data Breach Toolkit

Now more than ever, companies of all sizes, in all industries, need to be concerned about data privacy and security. Data breaches can have a devastating impact on your company's revenues, not to mention its reputation. And the true financial impact of a breach includes not just the expense of responding to the incident, but also the costs of defending the company in litigation and investigations by state, federal, and possibly foreign regulators.

Steptoe works to protect companies both before and after a data breach – from conducting pre-breach privacy and security assessments, to conducting tabletop exercises and breach simulations, to coordinating crisis management and incident response, to advising on breach notification, to defending companies in litigation and regulatory proceedings.

This toolkit is a resource to help companies evaluate their level of preparation for a breach. And for companies that are experiencing a breach, the toolkit will provide useful guidance on incident response and a reference on breach notification laws.

Data Breach Toolkit

- **Before a Breach Occurs**
  Engaging in a privacy and security assessment will help reduce your risk of a data breach while also putting your company in the strongest possible position to defend itself if a breach occurs.

- **After a Breach Occurs**
  A breach is a crisis, and as with any crisis, the company benefits from the assistance of skilled and experienced crisis counsel and advisors including forensics, IT, and corporate communications professionals.

- **Breach Notification Law Roadmap**
  The Breach Notification Law Roadmap summarizes the state and federal data breach statutes currently in effect.

To access this information online, please visit www.steptoe.com/databreach.

Before a Breach Occurs

PRIVACY AND SECURITY ASSESSMENT CHECKLIST

Engaging in a privacy and security assessment will help reduce your risk of a data breach while also putting your company in the strongest possible position to defend itself if a breach occurs. Critical components of a privacy and security assessment include the following:

✓ Network security

Technical security measures are a critical component of your overall level of protection, including, among other things:

- What type of authentication system and firewalls are in place?
- Are default passwords being used? Are passwords sufficiently strong, and are they changed regularly?
- If an employee leaves the company, is the employee's account on the network purged?
- Does the network have an intrusion detection or prevention system?
- Is encryption used on the network, and are mobile devices encrypted?
- Is logging enabled on your network, and are logs stored for a sufficient time?
- Is the company using up-to-date anti-malware protection?
- Does your company delete sensitive information when it is no longer needed?

✓ Incident response plan

If you don't have an incident response plan, you need one. If you have one, now is a good time to review it. Either way, that plan should be tested regularly so you know it will work when the time comes. A tabletop exercise or other breach simulation is a great way to find out if your plan works the way you drew it up. The plan should make clear who will be called in to help when an incident occurs, and your lawyer should be your first phone call. The lawyer in turn should engage the forensics firm and other outside experts. This increases the chance that your company will maintain the protection of the attorney-client privilege as it responds to the incident, which will be critical when litigation ensues.

✓ Identify and map your data

Make sure you know what data you have, and where it is. That will help you make decisions about how best to protect your data, evaluate compliance with applicable data security laws, and respond more efficiently and effectively if an incident occurs.

✓ Records retention policy

If you don't have it, it can't be stolen. So retain only the data the company needs for business operations; data that can be archived offline or destroyed, should be.

✓ Contracts with vendors/business partners

A vendor's network could be used as a launching pad for an attack on yours. Review your contracts with vendors and other business partners to ensure that they appropriately address responsibility and liability for data security, and that they provide for regular audits to ensure compliance.

✓ Employee training on cybersecurity

Data security is not just about technology; it's also about processes and people. Your employees are your first line of defense, but also a potential vulnerability. One employee who carelessly opens a spear-phishing email, allowing malware to get onto your network, can undermine millions of dollars in security investments. For that reason, reviewing and enhancing your training for employees, emphasizing their shared responsibility for cybersecurity, is critical.

✓ Privacy notices and practices

Do what you say, and say what you do. Compare your privacy notice with your company's practices to make sure you're actually doing what you say you're doing.

✓ Insurance coverage

No security is perfect, and the costs of a breach can be catastrophic, so ensuring that your insurance coverage is adequate – including response, remediation, and litigation costs – is critical to protecting your business.

✓ Access controls

Placing appropriate controls on access to data – including limiting access to personal and other sensitive information to only those employees who truly need it – will help mitigate the risk of attacks from both insiders and outsiders.

✓ Due diligence in M&A/other transactions

When you buy a company, you're buying its data. And you may be buying its data security problems. For that reason, cybersecurity should be a critical component of your due diligence.

After a Breach Occurs

INCIDENT RESPONSE CHECKLIST

A breach is a crisis, and as with any crisis, the company benefits from the assistance of skilled and experienced crisis counsel and advisors including forensics, IT, and corporate communications professionals. The following are critical components of effective incident response:

✓ Mobilize necessary personnel

- Legal
- IT
- Forensics
- Communications

✓ Containment and analysis

- Stem the damage
- Secure the network
- Preserve evidence
- Identify the source of the attack

✓ Notification

- Evaluate breach notification obligations
- Evaluate coordination with law enforcement/ regulators
- Corporate communications strategy

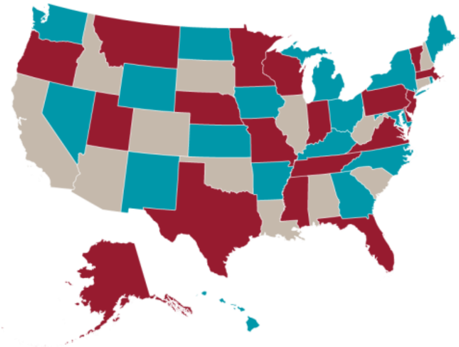
✓ Eradication and prevention

- After-action review
- Remediate security gaps
- Improvements to response policies and procedures

Breach Notification Law Roadmap

The Breach Notification Law Roadmap summarizes the state and federal data breach statutes currently in effect. Access the most recent version of the **Breach Notification Law Roadmap (pdf)** here.

**Please note that this summary is intended only to provide an overview of the various notification laws and does not constitute legal advice. In addition, the requirements of these laws can differ significantly, and they are subject to change over time. If you have questions about the possible application of any of these laws, please contact a Steptoe lawyer.*



Contacts

Stewart A. Baker
Partner
+1 202 429 6402
sbaker@steptoe.com

Michael Vatis
Partner
+1 212 506 3927
mvatis@steptoe.com

Jason M. Weinstein
Partner
+1 202 429 8061
jweinstein@steptoe.com

Alan Cohn
Of Counsel
+1 202 429 6283
acohn@steptoe.com