LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy, Security & Cybercrime Practice November 8, 2016 | Number 2029

5 Preventative Steps to Manage Legal Risk Following a Cybersecurity Breach

Preparing for and rehearsing how to respond to a breach is as important as improving security systems and protocols.

Hacking of organizations' systems is becoming increasingly commonplace, even with advancements in security practices. To mitigate risk, a company must have an enterprise-level, cross-functional incident response plan that is rehearsed and practiced. In the event of an incident a company with a rehearsed plan can avoid delays and mistakes, minimize conflicts between functions, and ensure regulatory, legal and contractual reporting requirements are met.

Companies and organizations across the globe face increasing threats of a security breach — both from internal threats (disgruntled employees or mislaid documents or laptops) and external threats (criminal networks, state-sponsored espionage and hacktivists). Breaches and other cybersecurity incidents can damage reputation and give rise to operational and legal risks, for example:

- Disruption of service (*e.g.*, due to distributed denial of service (DDoS) attacks)
- Interrupted payment processing (*e.g.*, due to breach of checkout terminals)
- Costs of investigation, remediation and notification
- Need for timely compliance with diverse and divergent domestic and foreign laws and regulations governing data breach notification
- Inquiries from regulators concerning the nature, scope, and cause of the breach, and investigations into the adequacy of pre-incident security measures
- Impact on share price following public disclosure of incident, where required
- Class actions or other private lawsuits brought by consumers, shareholders, or other affected parties
- Breach of contract disputes from customers and vendors

Take Preventative Action

No one can predict when or how a cybersecurity breach will occur, but organizations should take active steps to prepare. The following five actions can help ensure an organization's cyber-readiness.

1. Adopt and continuously optimize a formal cybersecurity program:

While any program should be tailored to industry and regulatory schemes, generally the program must have the following core components.

- Assign responsibility for cybersecurity to chief information security officer (CISO) or other senior executive

- Ensure board is engaged and regularly briefed on cybersecurity matters
- Establish written information security policies addressing relevant industry standards or regulations
- Periodically test and audit these policies and document follow-through

2. Conduct a risk assessment

- Identify the types of sensitive data you process and store
- Formally assess and inventory where on your systems sensitive data is held
- Identify threats and vulnerabilities to sensitive data
- Analyze how sensitive data is currently protected (how is risk being mitigated)
- Document costs/benefits of additional security measures, and agree upon a mitigation plan setting timelines and allocating necessary financial, personnel, and technical resources

3. Manage third-party risks

- Identify vendors and other third parties with access to or control over your systems or data
- Ensure third-party access is strictly limited to business need
- Develop procedures for conducting cybersecurity due diligence on vendors
- Review contracts with vendors to understand their obligations in the event of a breach

4. Train your employees

- Provide regular cybersecurity training to all employees (from top management down)
- Ensure employees understand relevant threats and good cyber hygiene practices
- Test employee understanding through realistic simulations (*e.g.*, mock phishing emails)
- Rehearse incident response plan with all relevant stakeholders

5. Develop and maintain an incident response plan

- Identify members of response team and define their roles (as discussed further below)
- Classify types of incidents that will trigger the plan and how they will be escalated internally
- Identify external parties that should be notified and articulate when/how notifications should be made
- Provide contact information for pre-vetted outside resources (external counsel, cyber-forensics firm)
- Refine plan based on lessons learned from each incident

Cross-Functional Incident Response Plan:

Define Roles and Responsibilities for Stakeholders

A company's incident response team should include all key stakeholders whose input or action will be needed as part of the response effort. Articulating each stakeholder's respective responsibilities ahead of time will facilitate quick decision-making and avoid internal conflicts. The following examples can help planning, but each organization will need to tailor team member roles to fit their specific structure and operations.

Information Technology

- Augment internal resources with outside experts if appropriate
- Ensure secure crisis communications portal
- Preserve relevant logs and systems to facilitate investigation
- Establish attack timeline
- Investigate attacker's means, motives and methods (including attack vector)

- Identify indicators of compromise (IOCs) and survey network for affected systems/data
- Determine whether sensitive data was accessed/acquired and assess scope of damage
- Manage containment/eradication
- Restore secure computing and remediate network

Legal Advisors

- Retain outside legal counsel if appropriate
- Ensure forensic, root cause, insider or other related investigations are conducted under umbrella of legal privilege
- Implement “legal hold” measures to preserve relevant evidence (in addition to any preservation activities undertaken by IT or forensic advisors on breached systems)
- Ensure timely notifications where required or prudent (to shareholders, regulators, consumers, etc.)
- Advise on internal and external communications to ensure accuracy and mitigate liability and regulatory risk
- Liaise with law enforcement and advise on any requests to collect evidence or monitor systems or employees
- Evaluate risk of liability related to adequacy of pre-breach measures and breach response
- Ensure response efforts are adequately documented in case of eventual legal scrutiny
- Prepare for potential legal action (lawsuits, regulatory inquiries)

Compliance/Regulatory

- Ensure response effort is carried out per plan and meets or exceeds required regulatory expectations
- Advise on notifying or otherwise contacting regulators regarding incident
- Assess any weaknesses in pre-breach controls and implement appropriate improvements
- Determine if pre-breach controls were not followed in practice and remediate performance gaps

Communications

- Develop communications strategy to minimize reputational damage and sustain customer loyalty
- Coordinate with human relations to advise employees about incident and what company is doing to respond

Investor Relations

- Prepare to answer questions about personnel, financial impact and costs of response and security upgrades
- Advise on whether to notify exchange if the company is listed
- Communicate with institutional investors directly and through associations expecting disclosures

Human Resources

- Advise on disciplinary actions if incident involves malicious or negligent employee conduct
- Respond to employee questions concerning the security of their personal information

Conclusion

Given the potential reputational, legal and financial fallout from a cybersecurity incident, thoughtful preparation and communication throughout an organization can deliver substantial and valuable benefits and minimize legal and reputation risk.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

Andrew Moyle
andrew.moyle@lw.com
+44.20.7710.1078
London

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York

Brian Meenagh
brian.meenagh@lw.com
+971.4.704.6344
Dubai

Madonna Kobayssi
madonna.kobayssi@lw.com
+971.4.704.6307
Dubai

You Might Also Be Interested In

New EU Data Protection Rules Move the M&A Goalposts

"Yarovaya" Law – New Data Retention Obligations for Telecom Providers and Arrangers in Russia

Are Changes in Store for the Stored Communications Act?

What You Need to Know About the Cybersecurity Act of 2015