SQUIRE SANDERS

HOW SAFE IS YOUR DATA?

Our Four-Point Data Breach Preparedness and Response Program

The Threat

As our data-driven economy evolves, the wonders of modern technology carry new challenges for business and consumers. Personal data and other types of sensitive electronic data have become a precious commodity. A company's reputation and fortunes can turn on a single data breach incident.

Comprehensive cyber risk insurance is still in its infancy. Issues surrounding the scope of coverage remain unresolved, with the potential exposure comparable to that for cataclysmic natural disasters. Prevention and rapid response are therefore the best insurance policies currently on offer.

Forward planning to minimize the risks associated with data breach incidents is no longer a matter for compliance professionals alone. Corporate boards and C-suite executives are now on the firing line. Shareholders are demanding action for companies up and down the line to take the measures necessary to: (1) properly secure data from loss, destruction and unauthorized access; and (2) respond effectively and without delay to data breach incidents that cannot be prevented.

Our Four-Point Program

Squire Sanders' Global Data Privacy & Protection Team includes data breach experts with a proven track record of advising clients on data breach preparedness and response at both the local and international levels. Our four-point program covers the essential elements of sound data management.

- **Prepare and Train**
- **Protect and Prevent**
- **Detect and Respond**
- **Recover and Fortify**

Our data breach experts regularly work together with technical security professionals on a range of action steps, including:

- review of local compliance requirements;
- development of compliance and prevention programs;
- drafting internal policies and processes;
- advising on due diligence to be undertaken with third party service providers and essential contractual terms;
- drafting tailored data breach response plans;
- carrying out internal data breach training;
- advising on how best to deal with data breach incidents including damage limitation, coordination with security consultants, notification to affected individuals and, where required, relevant governmental authorities;
- interfacing with investigating law enforcement agencies;
- coordination of crisis management with PR and IR professionals; and
- litigation preparation, strategy and defense.

Data Breach Checklist for Clients

Our Data Breach Preparedness Checklist provides a useful self-assessment tool for companies considering how to manage and limit the risk of accidental and intentional data loss or destruction, running the gamut from employees' lost laptops to advanced persistent threats and other hacking activities.

1. Prepare and Train

Compliance "Health Check"

☐ Have you identified all local, national and international compliance requirements that apply to your company?

☐ Have you carried out a compliance health check to evaluate how each relevant policy, procedure, security measure, communication, contract, training and monitoring activity:

- ☐ meets the relevant requirements, and
- ☐ safeguards personal data in a manner proportionate to the risk?

Internal Policies and Processes

☐ Does your company have internal policies in place covering email and Internet use/monitoring; information security; CCTV; and telephone and/or other monitoring?

☐ Are your employees fully aware of these policies?

☐ Are the policies regularly reviewed and updated?

☐ Do you conduct regular data protection training?

☐ Do you conduct periodic data breach incident response drills?

Risk Assessments

☐ Have you identified internal and external risks and vulnerabilities?

☐ If any third parties – ranging from payroll processors, cloud providers, website hosts or providers of software support, to archive and destruction contractors – have even incidental access to personal data:

- ☐ Have you done due diligence as to the security measures they have in place?
- ☐ Have you included the mandatory data protection requirements in your contract with them?
- ☐ Have you checked what obligations they have in the event of a data breach?
- ☐ Have you checked whether there are any indemnities, exclusions or limitations in relation to data breach?

☐ If your data is covered by state or federal data breach notification obligations and other requirements in the US, or if you store and process the personal data of EU residents:

- ☐ Do you have an inventory of all such data?
- ☐ Do you know which jurisdictions are potentially implicated?
- ☐ Do you know what each jurisdiction requires in terms of notifications to affected individuals and relevant government authorities, including the applicable deadlines?

Business Awareness

☐ Are your staff adequately trained to appreciate cyber risks, how to minimize the risk of a data breach and how to respond to a data breach incident should it occur?

☐ Is there a top down approach to data breach awareness across the business from board members and senior management to all other staff?

Data Breach Response Plan

- ☐ Does your company have a Data Breach Response Plan in place?
- ☐ Does your company have processes for both low and high risk incidents?
- ☐ Do you regularly ensure that roles and responsibilities, policies, procedures, tools and resources are up-to-date and still applicable?

Insurance

- ☐ Does your director's and officer's liability insurance cover cyber risk?
- ☐ Does your company's insurance cover cyber risk and have you assessed the scope of coverage in light of the risks your business faces?

2. Protect and Prevent

- ☐ Are your company's operations as secure as they can be/need to be? Have you considered:
  - ☐ Physical security, for example, CCTV and access permissions to IT security areas?
  - ☐ Technical security, for example, encryption measures and implementation of cyber-security standards?
  - ☐ Organizational security, for example, supervision and signoffs?
- ☐ Have you developed privacy by design features that embed monitoring tools, checklists, signoffs and/or certifications into areas identified as high risk?
- ☐ Have you assessed the legal and regulatory implications and risks of allowing employees to use their own devices and associated cloud providers?
  - ☐ Does your company have an effective, coherent and well-publicized Bring Your Own Device (BYOD) program in place?
  - ☐ Have you considered installing remote wiping tools and procedures for employee loss notification on all devices?
- ☐ Have you properly vetted the security measures implemented by any third party processors (including cloud providers) that your company uses?
- ☐ Has your company carried out a security audit of IT systems that process/store HR personal data?
- ☐ Does your company have the right to audit third-party vendors?

3. Detect and Respond

- ☐ Have you set up early warning alerts to rapidly detect and respond to data breach incidents?
- ☐ Are employees up and down the line aware of your Data Breach Response Plan?
- ☐ Have you identified a Crisis Response Team (internal and external) for dealing with data breaches, and are employees aware of who they are?
- ☐ Are you prepared to deal with the consequences of a serious data breach?
  - ☐ Technical
  - ☐ Commercial
  - ☐ Legal
  - ☐ PR/IR
- ☐ Are you prepared, if required, to notify all affected individuals of a data breach compromising their personal data, and deal with the questions/issues they raise?
- ☐ Are you prepared, if required, to notify all relevant governmental authorities in the jurisdictions affected and are you aware of local rules with regard to timing, form and content of the notification?
- ☐ Does your litigation department have a good working relationship with an external counsel expert in dealing with government investigations, prosecutions, class actions and shareholder derivative suits?

4. Recover and Fortify

- ☐ Is your company's data sufficiently backed up and can it be restored?
- ☐ Does your company have adequate business continuity measures in place in the event of a serious data breach?
- ☐ Do you have feedback loops in place to identify any changes required to address lessons learned?

If you would like further information on the services offered by our Global Data Privacy & Protection Team and how our data breach experts can assist, please contact:

Data Protection & Privacy

Ann LaFrance
Partner, London
T +44 20 7655 1752
E ann.lafrance@squiresanders.com

Philip Zender
Partner, San Francisco
T +1 415 393 9827
E philip.zender@squiresanders.com

Global Corporate

Laura D. Nemeth
Partner, Cleveland
T +1 216 479 8552
E laura.nemeth@squiresanders.com

David A. Zagore
Partner, Cleveland
T +1 216 479 8610
E david.zagore@squiresanders.com

Litigation

Colin R. Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squiresanders.com

Victoria Leigh
Partner, Manchester
T +44 161 830 5058
E victoria.leigh@squiresanders.com

Labor & Employment

Caroline Noblet
Partner, London
T +44 20 7655 1473
E caroline.noblet@squiresanders.com

Susan M. DiMickele
Partner, Columbus
T +1 614 365 2842
E susan.dimickele@squiresanders.com

12505/03/14