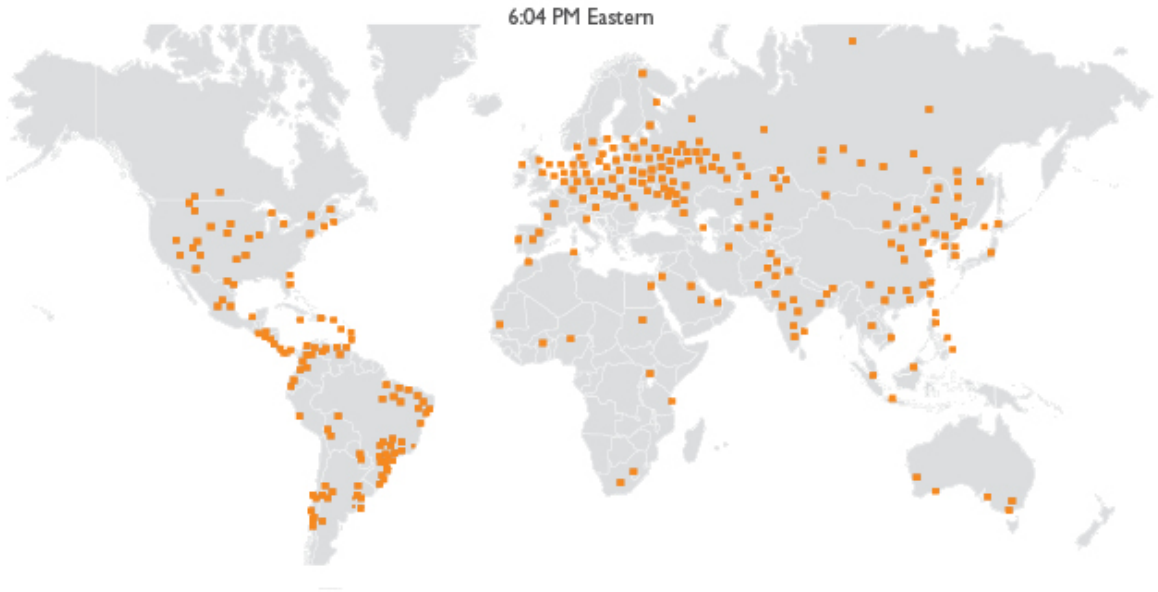
WannaCry ransomware attack was just the tip of the iceberg

9 things you should know to protect your company from the next attack

5 JUN 2017

By: Sammy Fang | Jason Chang



Source: Animated Map of How Tens of Thousands of Computers Were Infected With Ransomware - The New York Times, May 12 2017 - to see full article click here.

The WannaCry ransomware attack took the world by storm on Friday, May 12, 2017. By some accounts, the attack infected more than 200,000 computers in over 150 countries in a span of 24 hours. Law firms and cybersecurity experts have been teaming up for years to deal with the increasing number of cybersecurity threats by both proactively defending against cyberthreats through strengthened cybersecurity compliance as well as reactively pursuing cybercriminals around the world, working closely with law enforcement, courts, banks, and cyberexperts to help stop the loss of corporate funds and valuable data, and prosecute offenders. Cyberattacks are not going away anytime soon. We set out below some practical considerations and steps to help you prepare your company for the next attack:

1. **Early Stage Fact Finding:** Map data assets, compile key contracts and relevant obligations, tally up IT infrastructure and resources, review existing protocols and response plans, and check whether cybersecurity insurance is in place.
2. **Red-flag Review:** Identify legal obligations governing information handling and security, assess vendor management and data legal risks, identify regional differences in target countries, prepare checklist of breach notification obligations, ongoing legal review using customized review protocols which can provide regular alerts and updates on developments in regulation.
3. **Gap Analysis:** Report setting out weaknesses and deficiencies in cybersecurity/risk preparedness, Red Amber Green (RAG) report prioritizing rectification tasks in light of company culture and regulatory obligations, review company's governance structure as well as security policies and procedures.
4. **Development of Incident Response Plan:** This includes tabletop testing of the Incident Response Plan and refinement of the plan in light of the tests.
5. **Implementation:** Obtain advice on cybergovernance structure and reporting to C-suite and the board, rectification of RAG report deficiencies based on instructions, develop IT use protocols, cyber policies and procedures, personnel policies and level policies, maintenance of cyber systems and implementation monitoring, update contract methodology around cyber risk transfer and mitigation including vendor template agreements and vendor risk review process, establish business continuity and disaster recovery plans.
6. **Technology Support:** Engage a technology partner to support with penetration testing, setting encryption standards, and network infiltration health checks. Legal to support forensic review by scoping technology support requirements.
7. **Insurance:** Legal analysis of cyberinsurance options and coverage, identify exclusions and notification obligations, coverage review and preliminary advice on indemnity.
8. **Training:** Customized cybersecurity and threat training to C-suite to build awareness and management buy-in, conduct regular training to employees including training for key functions such as finance, legal and compliance, HR, and IT security as well as regular mock runs on incident response protocols.

9. **Incident Response:** If the company is a victim of an attack, time is of the essence. DLA Piper offers a 24/7 Rapid Response hotline and crisis management services for companies facing an immediate incident. Following an attack, the legal team will need to consider a variety of issues including managing technical forensic and PR consultants, advising on insurance coverage and notice obligations, reviewing rights and obligations in contracts with third parties, drafting breach notifications to regulators, individuals or card networks, and potential representation in regulator or payment card investigations or private lawsuits. Post-incident, the legal team should review the company's incident response plan and consider lessons learned.

DLA Piper has assisted numerous companies in strengthening its cybersecurity compliance, responding to incidents of data breaches and cybercrime, and recovering on behalf of these companies across the region and elsewhere around the globe. For further information regarding how we may assist with your company, please contact the authors.

Click to read our latest alert on the new PRC Cybersecurity Law.

DLA Piper's Data Protection and Privacy practice delivers topical legal and regulatory updates and analysis from across the globe. To learn more please click here.

AUTHORS

Sammy Fang
Partner
Hong Kong | T: +852 2103 0808
sammy.fang@dlapiper.com

Jason Chang
Of Counsel
San Francisco | T: +1 415 836 2500
Silicon Valley | T: +1 650 833 2000
jason.chang@dlapiper.com