SQUIRE PATTON BOGGS

Petya and Petya-like Attacks

The June 27, 2017 ransomware attacks appear to be rising to proportions similar to that of the WannaCry attacks last month.

No industry is entirely safe from these (temporarily) crippling attacks.

What can you do to manage today's attack or prevent it from affecting you?

Critical path at this point:

- **If you have been hit:**
  - For any systems that have not been hit, immediately apply patches issued to address the ETERNALBLUE exploit
  - Make sure to stop the spread of the attack – do not overlook systems that have not yet been compromised
  - Identify which of your systems should be isolated or kept offline based on particular indicators known to be part of the Petya or Petya-like Attack
  - Determine the best path for recovery as quickly as possible
- **If you have not been hit:**
  - Apply patches to stop the ETERNALBLUE exploit available here
  - There is still time to prevent the attack using certain forensic sensors
  - Watch media coverage for additional indicators of the attack and remain vigilant for additional attacks

How We Can Help Immediately

- Revise and redirect your current response effort
- Ensure you have the best advice from forensic or technical experts
- Ensure technical response is comprehensive and legally defensible in any later investigations
- Advise on executive decisions regarding whether or not and/or how to pay ransomware
  - As of midday June 27, current advice being reported in the media is not to pay
- Engage a specialty PR/communications firm to assist with reputational and brand management (internally and externally)
- Consider whether privilege is appropriate or necessary under applicable law; ensure privilege established with communications/PR and forensic vendors
- Apply privilege to remedial efforts where possible
- Advise on liability exposure throughout the response effort
- Assist with helping ensure you avoid a second attack over the next few weeks on the heels of this one
- Handle regulator inquiries, customer inquiries, etc.
- Coordinate with law enforcement if necessary

Our Data Privacy & Cybersecurity Team

Our Data Privacy & Cybersecurity team is a rapidly growing group of some of the most seasoned cybersecurity and privacy partners in the world. Of particular relevance to today's events, we have significant expertise and can assist you and your organization in preparing for or recovering from crippling cyberattacks.

- Represented clients in over 200 crisis responses in data security incidents
- Frequently run forensic investigations and assist with technical planning and mitigation to minimize liability exposure
- Ran incident responses for multiple of the largest worldwide data breaches:
  - Coordinated forensic investigation direction and information-gathering
  - Handled PR and communications response, including media messaging and communications with cyber bloggers attempting to blackmail company and users
  - Liaised with law enforcement and regulators in multiple countries
  - Defended clients in federal and state enforcement actions
- Worldwide expertise, experience and collaboration
- Former Department of Justice cybercrime prosecutor

Companies in heavily regulated industries, such as financial services, may have additional, industry-specific regulatory compliance and reporting obligations. Our Data Privacy and Security team works closely with attorneys on our regulatory team to ensure comprehensive, proactive compliance with industry-specific regulations and the maintenance of regulatory relationships, as appropriate.

Contacts

Tara Swaminatha
Partner, Washington DC
T +1 202 457 6031
E tara.swaminatha@squirepb.com

Robin Campbell
Co-Lead, Data Privacy & Cybersecurity
Partner, Washington DC
T +1 202 457 6409
E robin.campbell@squirepb.com

Ann LaFrance
Co-Lead, Data Privacy & Cybersecurity
Partner, London
T +44 20 7655 1752
E ann.lafrance@squirepb.com