What companies can do

Tips on cybersecurity and public relations in the event of a cyberattack

Cybersecurity

- Establish a secure architecture that uses advanced cybersecurity defence technologies
- Promptly install important software updates; fully patch all systems
- Back up critical systems' files, and keep that backup offline
- Segment networks and implement air gaps where appropriate to limit spread of malware
- Automatically block all corporate connections to known malicious IP addresses using a continuously updated threat intelligence feed
- Don't execute attachments from unknown sources
- If affected, don't pay the ransom. Share facts of infiltration with trusted organisations (eg, local police) to assist with overall community efforts to diagnose, contain and remedy the attack

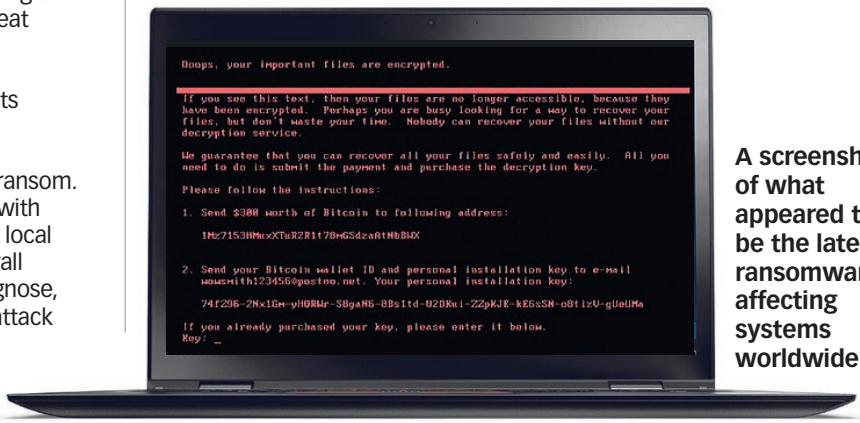
Public relations

Get it fast:
Make sure you know internally when a cyberattack happens. Prepare a communications strategy before you get hit

Get it right:
Find out what exactly happened and what's been done to mitigate the situation

Get it out:
Don't wait to share what you know – be transparent and avoid any speculation. It's okay not to have all the answers at the beginning of a crisis

Get it over:
Assure stakeholders and wider audiences that you are in control of the situation, working on the matter, and will learn from it



A screenshot of what appeared to be the latest ransomware affecting systems worldwide

Source: ESET, FireEye, Fortinet, McAfee, Lars Voedisch (PRecious Communications)