the Availability Digest

www.availabilitydigest.com
@availabilitydig

Should Cyber Victims Be Fined?

August 2017

Just the title of this paper seems absurd. Should cyber victims be fined? They have already suffered from a cyberattack. Why should they be made to suffer further?

But this is exactly what the U.K. is doing. It is responding in part to the £60 million cyberattack on TalkTalk in 2015

'Essential' Infrastructure Operators

'Essential' infrastructure operators could be fined £17 million or four percent of profits if they suffer an outage because of insufficient security. Essential providers include those in the utilities, health, transport, and communications sectors.

The potential fines for essential infrastructure operators are driven by the U.K.'s new Network and Information Systems (NIS) directive. They are part of a Department for Digital, Culture, Media, and Sports (DCMS) initiative to implement the NIS directive. DCMS said the fines would be a last resort and would not apply to those who had taken every conceivable measure, yet still suffered a cyberattack.

One of the biggest problems with data breaches caused by cyberattacks is how the data is used. Malicious attackers can use the data to construct emails that appear to be from appropriate sources to get unsuspecting users to divulge private information, to change passwords, or to update PINs that are now known to the attackers.

The TalkTalk Cyberattack

TalkTalk is the U.K.'s second largest communication service, offering TV, broadband, phone, and mobile services. As such, it is an essential infrastructure operator.

In October, 2015, TalkTalk suffered a devastating cyberattack. A consequence of this attack was that it lost 95,000 subscribers. As a result, profits slumped from £72 million in 2015 to just £2 million in 2016. The company lost up to £60 million in revenue and in exceptional costs required to recover from the cyberattack.

The National Cybersecurity Center

The U.K. has issued the Network and Information Systems (NIS) directive requiring organizations to use best practices for implementing cybersecurity. The fine proposals form part of the motivation for companies to conform to the NIS directive.

The U.K. has also created the National Cybersecurity Center (NCSC) to help organizations in this task. The NCSC, which is part of the government's £1.9 billion National Cybersecurity Strategy, has welcomed the fine proposals.

Minister for Digital Matt Hancock said "We want the UK to be the safest place in the world to live and be online, with our essential services and infrastructure prepared for the increasing risk of cyberattack and more resilient against other threats such as power failures and environmental hazards.

"The NCSC is committed to making the UK the safest place in the world to live and do business online, but we can't do this alone. Everyone has a part to play, and that's why since our launch we have been offering organizations expert advice on our website and the Government's Cyber Essentials Scheme."

Shoring Up Defenses

Clearly, companies need to shore up their defenses against cyberattacks. This includes web defenses, encryption, firewalls, web filtering, and ongoing threat monitoring. They need to make sure that they have network visibility of information and those accessing it while the data is stored, on the move, or taken off the network. This is the first line of defense against any potential attack.

The WannaCry attacks on the public health systems show how cyberattacks can have debilitating consequences.[1] Security is often an afterthought. Hopefully the news of such fines will wake organizations up to the seriousness of the consequences from a financial viewpoint, never mind a reputational one.

The notion that executives be involved in cybersecurity is essential. The implications and remedies of cybersecurity issues cut across every aspect of an organization's operations.

Education of a company's employees is very important:

- How can they protect your company?
- If your company is breached, how can they help your customers mitigate the damage that occurs?
- How can they tell if an email is really from who it is purported to be?
- How can they be sure that a web site that asks for their credentials really belongs to your service provider?
- How can they tell if a tweet from your bank asking them to reset their PIN code is legitimate?

Summary

The U.K. is taking extreme measures by threatening to fine essential infrastructure operators who suffer a cyberattack. It will be interesting to follow this measure to see if it encourages companies to make further investments in combating cybercrime.

[1] WannaCry Global Ransomware Attack, *Availability Digest*; June 2017.
http://www.availabilitydigest.com/public_articles/1206/wannacry.pdf

Acknowledgements

Thanks to our subscriber, Terry Critchley, for referring us to this story. Information for this article was taken from the following sources:

TalkTalk Eyes Business Fibre And Mobile Growth As Cyberattack Hangover Continues, *Silicon*; May 12, 2016.
Will MPs' TalkTalk Hack Recommendations Make the UK More Secure?, *Silicon*; June 20, 2016.
Businesses Face Fines if Cyberattack Causes 'Essential' Service Changes, *Silicon*; August 8, 2017.
Security Panel: Will Threat Of Fines For Poor Cybersecurity Have An Impact?, *Silicon*; August 8, 2017.